E-Deceptive Campaign Practices Report 2010:

Internet Technology & Democracy 2.0

Electronic Privacy Information Center

epic.org
ELECTRONIC PRIVACY INFORMATION CENTER

Contents

Executive Summary

In 2008, EPIC identified electronic deceptive campaign tactics as a high priority voter privacy issue. EPIC released the E-DECEPTIVE CAMPAIGN PRACTICES REPORT: INTERNET TECHNOLOGY & DEMOCRACY 2.0, which examined the potential for deceptive campaigns that used Internet communication services.[1] In 2010, the potential for deceptive election tactics and Internet information services remains. This update provides new insights and offers recommendations on what Election Administrators, poll workers, Election Protection, and voters may do to address threats to free and fair elections in the United States.

Deceptive campaigns are attempts to misdirect targeted voters regarding the voting process or in some way affect their willingness to cast a vote. Deceptive election activities include false statements about poll place opening and closing times, the date of the election, voter identification rules, or the eligibility requirements for voters who wish to cast a ballot. The goal of deceptive campaigns is, by attrition, to reduce the total number of voters who would without interference cast a vote in a public election. Voter suppression activity is believed to be most effective in disrupting voters' participation in elections that are highly contested. Over time, some voting blocks may have demonstrated preferences that could decide the outcome of very close elections. These voters may be deemed to be non-persuadable and their participation could influence the final results of an election.

Historically, disinformation and misinformation efforts have been intended to suppress voter participation among low-income, racial and language minorities, young, disabled, and elderly voters.[2] The current foreclosure crisis has also presented opportunities for disinformation about voting rights.[3] Homeowners, who are either going through the foreclosure process or who have been foreclosed upon, should know that they are most likely still eligible to vote at their home or former home's polling place.[4]

---

[1] Computers Freedom and Privacy, Tutorial, E-Deceptive Campaign Practices 2.0, May 20, 2008, http://www.cfp2008.org/wiki/index.php?title=E-Deceptive_Campaign_Practices:_Elections_2.0&redirect=no; *see also* EPIC, E-DECEPTIVE CAMPAIGN PRACTICES REPORT: INTERNET TECHNOLOGY & DEMOCRACY 2.0, October 2010, *available at* http://votingintegrity.org/pdf/edeceptive_report.pdf.

[2] Brian Freeman, Michael Fields, Raymond Rodriguez, VOTER SUPPRESSION: *NEW HAMPSHIRE'S RESPONSE TO A NATIONAL PROBLEM*, The Center for Public Policy and the Social Sciences, Rockefeller Center at Dartmouth College, March 9, 2009, http://rockefeller.dartmouth.edu/shop/#fy11briefs.

[3] Editorial, "Foreclosures and the Right to Vote," nytimes.com, October 5, 2008, *available at* http://www.nytimes.com/2008/10/05/opinion/05sun2.html; Eartha Jane Melzer, "Lose Your Home, Lose Your Vote," *The Michigan Messenger*, September 10, 2008, *available at* http://michiganmessenger.com/4076/lose-your-house-lose-your-vote.

[4] Fair Elections Legal Network, LOSE YOUR HOME, KEEP YOUR VOTE: HOW TO PROTECT VOTERS CAUGHT UP IN FORECLOSURE, September 1, 2010, http://www.fairelectionsnetwork.com/index.cfm?fuseaction=page.viewpage&pageid=723.

Deceptive techniques have typically relied on telephone calls, ballot challenges, direct mail, and canvass literature drops to keep voters from the polls.[5] The increasing vitality of Internet-based communications to engage voters, and the concomitant governance challenges associated with the Internet, require voters to be aware of new ways in which their votes might be suppressed. On Election Day in 2008, the George Mason University Provost's email was hacked. Using that email address, hackers sent a university-wide "update" to students that Election Day had been moved to the following day.[6] Incidents such as this show that deceptive practices that target e-mail, instant messaging, and cell phone users can compress the timeline for launching successful disinformation and misinformation attacks from days to hours or minutes.

A major challenge for voters this election season is the effect of large sums of untraceable funds entering the political process that may be used to develop unique and more effective deceptive campaigns.[7] Messages intended to suppress or discourage voter participation may come from digital wolves dressed in social networking sheeps' clothing.

Most notable activity in 2010:

- In September 2010, Maryland's Attorney General obtained a restraining order to halt the distribution of a fraudulent and deceptive campaign ballot distributed in Prince George's County.[8]

- Special interest group spending up five fold over what was spent in 2006, the last mid-term Congressional federal election. In 2010, many of these sources of additional campaign-related funding remained secret.[9]

This report reviews the potential for abuse of Internet technology in the election context, and makes recommendations on steps that could be taken by Election Protection, Election Administrators, and voters to protect the right of citizens to participate in free and fair elections in the United States.

Appendix A of the report defines malicious software (viruses, worms, Trojan horses, or rootkits) and provides action steps for protecting personal computers.[10] Appendix B provides

---

[5] Election Protection, Incidents of Deceptive Practices and Voter Intimidation in the 2006 Elections, *available at* http://lccr.3cdn.net/d6af26cb31ff5ee166_vdm6bx6x5.pdf.

[6] "GMU E-Mail Hoax: Election Day Moved to Nov. 5," The Washington Post, *available at* http://voices.washingtonpost.com/securityfix/2008/11/gmu_e-mail_hoax_election_day_m.html.

[7] Ruth Marcus, "Court's campaign finance decision a case of shoddy scholarship," Washington Post, January 23, 2010. http://www.washingtonpost.com/wp-dyn/content/article/2010/01/22/AR2010012203897.html

[8] Maryland Attorney General's Office, "Attorney General Gansler Obtains Restraining Order Halting Distribution of Fraudulent Campaign Ballot," September 7, 2010, http://www.oag.state.md.us/Press/2010/090710.htm.

[9] T.W. Farman and Dan Eggen, "Internet-Group spending from midterm up fivefold from 2006; many sources secret," May 4, 2010, http://www.washingtonpost.com/wp-dyn/content/article/2010/10/03/AR2010100303664.html.

an E-Deceptive Campaign Practices Technology Checklist regarding the potential harm to voting by spoofing, phishing or pharming, denial of service, rumor-mongering, or social engineering campaign threats.[11]

For comments or questions regarding this technology report:

Lillie Coney
Electronic Privacy Information Center
202-483-1140 x111
http://epic.org/

Nichole Rustin-Paschal, Ph.D., J.D.
Open Government Fellow
Electronic Privacy Information Center
202-483-1140
http://epic.org/

[10] EPIC, E-DECEPTIVE CAMPAIGN PRACTICES REPORT: INTERNET TECHNOLOGY & DEMOCRACY 2.0, Appendix A, October 2010.
[11] EPIC, E-DECEPTIVE CAMPAIGN PRACTICES REPORT: INTERNET TECHNOLOGY & DEMOCRACY 2.0, Appendix B, October 2010.

Report Contributors

Lillie Coney is Associate Director with the Electronic Privacy Information Center (EPIC) in Washington, DC. She is currently serving on the Election Assistance Commission Board of Advisors. She contributed to the Brennan Center Taskforces on the Security and Usability of Voting Systems. She also served as a member of the ACM Committee on Guidelines for Implementation of Voter Registration Databases. She contributed to the academic paper "Towards a Privacy Measurement Criterion for Voting Systems."

Peter G. Neumann has doctorates from Harvard and Darmstadt. After 10 years at Bell Labs in Murray Hill, New Jersey, in the 1960s, he has been in SRI's Computer Science Lab since September 1971. He is concerned with computer systems and networks, security, reliability, survivability, safety, and many risks-related issues such as voting-system integrity, crypto policy, social implications, and human needs including privacy. He moderates the ACM Risks Forum.

Jon Pincus is writing Tales from the Net (a book on social networks co-authored with Deborah Pierce and his brother Greg), launching a strategy consulting practice achangeiscoming.net, and Vice-chair of online visibility for the Computers, Freedom, and Privacy (CFP) conference. Previous work includes leading the Ad Astra (Analysis and Development of Awesome STRAtegies) project as General Manger for Strategy Development in Microsoft's Online Services Group; creating the static analysis tools PREfix and PREfast (now available in Visual Studio) at his startup Intrinsa and then at Microsoft Research; security planning with the Windows Security Push and XPSP2 task forces; and the National Academies/CSTB panel Sufficient Evidence. Jon spoke on e-Deceptive practices at this year's CFP, and blogs about voting rights as well as other political and technical issues on his blog Liminal States.

Editors

Nichole Rustin-Paschal
Open Government Fellow
EPIC

Sharon Goott Nissim
Consumer Protection Fellow
EPIC

Introduction: Internet Communications and Deceptive Campaigns

Voters are firmly on the road to a new form of one-to-one political activism because of the Internet. The ubiquity and low cost of the Internet makes it ideal for mass communication. Individuals, governments, partisans, and multi-national organizations use the Internet to engage and be engaged in the political process. The Internet has profoundly changed the ability of citizens to participate in public elections.

In 2004, the Internet was first used as a major organizing tool for modern democracy and pubic engagement.[12] Internet communications were used to engage new voters, raise funds, and organize individuals for civic participation. By 2008, election officials were using the Internet as a tool to enhance the information services provided to voters. Election protection efforts were using the Internet as a means of informing voters of their rights, coordinating activities of volunteers, and providing near real time feedback of Election Day events. Campaigns were using the Internet as a more efficient means of targeting voters for messaging and solicitation of financial support as well as organizing. Today, in addition to telephone outreach, campaigns, organizers, and voters create or rely upon Web pages, blogs, e-mail, instant messaging, and YouTube to receive or get out their election messages. Individual voters are empowered by the Internet to speak directly to the electorate, candidates, and policymakers through their own messaging, bypassing traditional media outlets such as television, radio, and newspapers.

Deceptive campaigns are attempts to misdirect targeted voters regarding the voting process. Deceptive election activities include false statements about polling times, the date of the election, voter identification rules, or the eligibility requirements for voters who wish to cast a ballot. There are deceptive campaign messages that are specifically designed for particular audiences, which can impact voter participation. For example, media reports or e-mail blasts that inaccurately state the potential for voter fraud could be designed to influence poll worker conduct on Election Day toward certain blocks of voters such as youth, minorities, new citizens, or minority language speakers.[13]

The goal of deceptive campaigns is, by attrition, to reduce the total number of voters who would support a particular political party, candidate, or outcome on a ballot initiative. Voter suppression is key to stopping voters because certain identifiable blocks of voters are known to cast their ballots in a predictable way.[14] For example, in 2008 black women had the highest voter participation of any voting block for the first time.[15] Exit polls from the general election

---

[12] *See* Gary Wolf, "How the Internet Invented Howard Dean," wired.com, January 2004, http://www.wired.com/wired/archive/12.01/dean.html.

[13] Justin Levitt, THE TRUTH ABOUT VOTER FRAUD, Brennan Center for Justice http://www.truthaboutfraud.org/pdf/TruthAboutVoterFraud.pdf.

[14] Phillip Elliott, "Warnings of voter suppression," *Washington Post,* October 14, 2010, http://www.washingtonpost.com/wp-dyn/content/article/2010/10/14/AR2010101400853.html.

[15] Pew Center Research Publication, DISSECTING THE 2008 ELECTORATE: MOST DIVERSE IN U.S. HISTORY, April 30, 2009, http://pewresearch.org/pubs/1209/racial-ethnic-voters-presidential-election.

in 2008 show that 95% of black voters, of which black women constituted a higher percentage than black men, voted for Barack Obama.[16]

Voters who are targets of deceptive campaign tactics are generally non-persuadable voters and their participation could alter the outcomes for an election. EPIC's report examines the most likely forms of electronic deceptive campaign tactics and provides strategies for combating them.

Voter Profiling and Targeted Campaigns

An important aspect of Internet-based election deceptive campaign attacks is the ability of attackers to effectively identify targets for messages. Voter profiling for targeting campaign messages is nothing new. For decades, campaigns have collected information in order to create profiles. Campaigns collect this data from voter registration applications, voters' history of participation, state-issued professional licenses, and low-level elected office holders. Profiles are used to develop expectations regarding the behavior of individuals based on their activities, preferences for a wide range of products and services, personal associations, religious beliefs, past political participation, type of work, neighborhood, place of birth, and level of education.[17] In 2010, the list of voter profiling categories could include active military service membership, foreclosure status of a primary home, employment status, as well as emotional or mental state regarding the economy.

Few voters are aware of how much information about the details of their lives is in the hands of third parties.[18] Law enforcement, businesses, and political campaigns are making great progress in mastering the ability to create detailed profiles on individuals.[19] Each of the major political parties and their candidates are spending billions of dollars in the race to gain greater knowledge of the voters they seek to persuade. In 2006, it was reported that Voter Vault, political software developed by Filpac, a Republican firm, contained data on 160 million Americans.[20]

---

[16] Claire Cohen, "Breakdown of demographics reveals how black voters swept Obama into White House," *Daily Mail*, November 5, 2008, http://www.dailymail.co.uk/news/worldnews/article-1083335/Breakdown-demographics-reveals-black-voters-swept-Obama-White-House.html.

[17] Bill Blaemire, Catalyst LLC, "Campaigns and Voter Profiles," December 29, 2009, http://www.c-spanvideo.org/program/290960-3.

[18] T.W. Farnam and Dan Eggen, "Interest-group spending for midterm up fivefold from 2006; many sources secret," *The Washington Post,* October 4, 2010, *available at* http://www.washingtonpost.com/wp-dyn/content/article/2010/10/03/AR2010100303664.html.

[19] Jacqui Cheng, "Govt relies on Facebook 'narcissism' to spot fake marriages, fraud," October 2010, arstechnica.com, *available at* http://arstechnica.com/tech-policy/news/2010/10/govt-takes-advantage-of-facebook-narcissism-to-check-on-users.ars*; see also* Michael D. Shear, "Va. Gubernatorial Hopefuls Use Data to Zero In On Voters," CO1, *Washington Post*, August 28, 2005, *available at* http://www.washingtonpost.com/wp-dyn/content/article/2005/08/27/AR2005082700990_pf.html.

[20] Thomas Fitzgerald, "Parties pin hopes on voter profiling," *Bradenton Herald,* 3, November 2, 2006; *see also* http://www.filpac.com/votervault.htm.

Consumer profiles are major currency in electronic commerce where advertisers and marketers predict a user's preferences, interests, needs and possible future purchases using these profiles.[21] Retailers routinely share or sell data on customers and have used that information to improve products and services. Now, retailers are sharing or selling that information to data brokers who use the information to create rich profiles on consumers.[22] Many of these profiles are currently stored in connection with an assigned number or the user's Internet Protocol (IP) address.

Consumer profiles expose users to the risk of being linked to other information, such as names and addresses, making the user personally identifiable. The risks became all too real when, in 2006, America Online (AOL) made the search records of 658,000 Americans public. Although the search logs released by AOL had been "anonymized," identifying users only by assigned numbers, news reporters easily matched user numbers with identifiable individuals.[23]

Consumer profiles are also now coupled with Internet data collection to build detailed voter profiles that could be used to engage voters in the political process. The 2008 Presidential Election was the first in which the candidates used behavioral targeting to pinpoint voters.[24] Democratic and Republican campaign experts are also using micro-targeting to mine voter registration information and consumer data to build the perfect voter profile.[25] For example, TargetPoint Consulting provides micro-targeting services that combine consumer data, marketing techniques, and traditional political targeting to guide political campaigns. The company provides a "data-rich resource to guide a campaign's strategic decision-making."[26] Micro-targeting, according to the company, is a tool "that helps to answer their [customers'] most fundamental questions: Who supports my candidate? Where do I find them? How do I persuade others to support my candidate? When should I talk to them? Who should my messenger be?"[27]

---

[21] Representative Ed Markey, Oct 8, 2010-Markey, Barton Release Responses from Web Sites on Their Tracking of Consumer Behavior (press release with copies of responses), October 8, 2010, *available at* http://markey.house.gov/index.php?option=content&task=view&id=4103&Itemid=125.

[22] Jennifer Slegg, "What's the Buzz Behind Behavioral Advertising," *Search Engine Watch*, May 11, 2006, http://searchenginewatch.com/3605361; *see also* "Behavioral Targeting to Grow," *Adweek*, February 18, 2010, http://www.adweek.com/aw/content_display/news/digital/e3iccd499946ba0cc761fcc25e25943c52e.

[23] EPIC and Privacy International, PRIVACY AND HUMAN RIGHTS, 2006.

[24] Heather Green, "The Candidates Are Monitoring Your Mouse," *Bloomberg Business*, August 28, 2008, http://www.businessweek.com/magazine/content/08_36/b4098022877194.htm.

[25] Thomas Fitzgerald, "Profiling is key to '06 turnout; Campaigns are mining consumer data for votes," *The Philadelphia Inquirer*, A01, October 29, 2006.

[26] TargetPoint Consulting, *available at* http://www.targetpointconsulting.com/ToThePoint/2010/08/25/4-ways-location-data-can-change-campaigns.

[27] TargetPoint Consulting, Helping to Better Understand MicroTargeting, *available at* http://www.targetpointconsulting.com/system/uploads/14/original/MicroTargeting_101_8-2009.pdf?1249570076.

Aristole is another company specializing in election services for candidates, characterizing its work as mapping "the DNA of the electorate." The company claims that for 25 years every elected occupant of the White House has relied on their voter matching services. The company touts its ability to provide campaigns with 24/7 access to voter by using its VoterListsOnline.com service. The service allows campaigns to "select and target only the voters you need by targeting individuals through a comprehensive selection of demographics including but not limited to: political district, political party affiliation, Super-voters, gender, ethnicity, marital status, wealth, educational level and presence of children."[28]

Internet data collection is pervasive and completely hidden from online users. Many companies, including Internet Service Providers (ISPs), search engine firms, and web-based businesses monitor users as they travel across the Internet. These companies collect information on what sites users visit, the time and length of these visits, search terms they enter, purchases they make, or even "click-through" responses to banner ads.[29] In the off-line world this would be comparable to someone following you through a shopping mall and scanning each page of every magazine you browse though, every pair of shoes that you look at, and every menu entry you read at the restaurant. When collected and combined with other data, such as demographic or "psychographic" data,[30] these diffuse pieces of information create highly detailed profiles of individuals. These same consumer profiles could be used to develop much more sophisticated voter suppression tactics.

In the past, deceptive campaigns have relied upon knowledge about the demographics of communities to deliver deceptive mail pieces, flyers, or door-to-door literature. Later, voter registration information, coupled with telephone numbers, allowed deceptive campaigns to better target messages and have greater assurance that the intended recipient of the message received the communication. Past deceptive campaign practices include:[31]

- In September 2010, Maryland's Attorney General obtained a restraining order to halt the distribution of a fraudulent and deceptive campaign ballot distributed in Prince George's County.[32]

---

[28] Aristotle, VoterListsOnline.com, *available at* http://www.aristotle.com/content/view/35/119/.
[29] *Behavioral Advertising: Industry Practices And Consumers' Expectations: Hearing before the House Committee on Energy and Commerce, Subcommittee on Commerce, Trade, and Consumer Protection, and the Subcommittee on Communications, Technology, and the Internet*, June 18, 2009 (statement of Jeff Chester, Center for Digital Democracy), *available at* http://www.democraticmedia.org/doc/cdd-testimony-20090618.
[30] Andrew Tjan, "Want to Understand Your Customers? Go Psycho," *Harvard Business Review*, May 28, 2009, http://blogs.hbr.org/tjan/2009/05/want-to-understand-your-custom.html.
[31] Demos, "Voter Suppression Tactics Could Mar 2006 Election, New Publication Finds," http://www.demos-usa.org/press.cfm?currentarticleID=842B35AD-3FF4-6C82-5C57AADA7E3B9DDD.
[32] Maryland Attorney General's Office, "Attorney General Gansler Obtains Restraining Order Halting Distribution of Fraudulent Campaign Ballot," September 7, 2010, http://www.oag.state.md.us/Press/2010/090710.htm.

- In North Carolina in 2008, robo-calls were directed to predominately African-American households, telling them that before they could vote, adults needed to return the voter registration packet they received in the mail.[33]

- In 2008, campaign fliers using photo-shopped images and misrepresenting the politics of candidates were handed out to black voters on Election Day at Virginia Beach, Virginia polling places.[34]

The use of new technology for deceptive campaign tactics significantly increases the number of potential victims. Further, the ability to identify a deceptive campaign may be more difficult because of the very nature of Internet communications and social networking services. Technology enables and expands the opportunity to participate in elections, but it also offers tools to those who may wish to dissuade voters from casting ballots in elections. For example, as telephone service became common, deceptive campaigns adopted the technology to launch attacks. It is reasonable and prudent to extrapolate that, as voters, campaigns, discussion forums, and election administration services transition to the Internet, deceptive campaigns will as well.[35]

The Challenges of Internet Enabled Political Participation

Internet political communications may make the application of existing state and federal laws intended to regulate political activity more challenging to enforce. In the case of deceptive political Internet communications, the challenge of identifying the source, and more importantly, enforcing state and federal laws intended to protect citizens from deceptive election practices, will require new approaches. More state legislatures are amending campaign financing laws to account for the effect of Internet technology on political advertising.

For example, under Florida state law, political advertisements must include an attribution that discloses that the ad is in fact a political advertisement, who paid for the ad, whether it was approved by the candidate, and what office the candidate is seeking. Google AdWords allows users to create ads and choose keywords that will allow the user's ad to appear when an individual searches Google using those keywords.[36] In 2009, Scott Wagman, mayoral candidate in St. Petersburg, Florida, purchased a Google AdWords advertisement that appeared

---

[33] "Elections board hunting robocaller," *News Observer*, April 28, 2008, http://projects.newsobserver.com/under_the_dome/elections_board_hunting_robocaller.

[34] Diedre Fernandes, "Oberndorf campaign files complaint on Sessoms-Obama flier," *The Virginia-Pilot,* November 29, 2008, http://hamptonroads.com/2008/11/oberndorf-campaign-files-complaint-sessomsobama-flier#rfq.

[35] Alex Koppelman, "Voter suppression in North Carolina?," Salon.com, http://www.salon.com/politics/war_room/2008/05/02/robocalls/.

[36] Google, Google AdWords, https://www.google.com/accounts/ServiceLogin?service=adwords&hl=en_US&ltmpl=adwords&passive=true&ifr=false&alwf=true&continue=https://adwords.google.com/um/gaiaauth?apt%3DNone%26ugl%3Dtrue&gsessionid=XzEXIY8CHECcOnfqpbS0nw.

in search results any time someone searched for his opponents' names.[37] Because of the character limitations on GoogleAds, the full disclaimer was not included in the ad. Wagman was fined $250 for violating the law, but a subsequent lawsuit threw out the fine.[38] Florida law now makes an exception to the disclosure requirement when ads are placed online.[39]

A primary purpose of the early Internet was to allow for the quick dissemination of results among researchers.[40] Hence, it was designed to be robust and efficient. However, because only a small community of researchers and scientists with well-defined roles used it, security was not a major concern. Even as it became accessible more broadly to users and grew considerably in the nature of its scope and its uses, the intent remained the same: to allow for efficient communication, unhindered by administrative restrictions. The nature of the network makes it particularly difficult for an individual entity to supervise—a phishing site can shut down immediately, leaving very little information about its owner and his or her geographical location.[41]

The fact that the Internet is spread across the world provides another challenge to legal regulation.[42] This absence of regulation has served the Internet well in the past, allowing for explosive growth and the possibility of efficient communication among individuals across the globe. However, the lack of regulation of the Internet has presented problems for consumers in having control of personal information. The Internet environment could present problems for enforcing voting rights and thwarting voter suppression efforts that take advantage of this medium.

The enforcement of campaign regulations regarding political mail and telephone communications would likely be very intrusive in cyberspace unless designed carefully and supported by the active participation of users, nonprofits, governments, and commercial interests.[43] However, government policy regarding online credentials and registration of

---

[37] National Conference of State Legislatures, "Internet Campaigning." Septembr 7, 2010. http://www.ncsl.org/default.aspx?tabid=21244

[38] Zachary Rodgers, "Florida Politico to Fight Complaint on Use of Search Ads," *ClickZ: Marketing News & Expert Advice*, August 11, 2009, http://www.clickz.com/clickz/news/1713930/florida-politico-fight-complaint-use-search-ads.

[39] Kate Kaye, "Florida's New Political Ad Law Could Drive Dollars from State Candidates Online," *ClickZ: Marketing News & Expert Advice*, June 2, 2010; *see also* National Conference of State Legislatures, available at http://www.ncsl.org/default.aspx?TabId=21244, http://www.clickz.com/clickz/news/1726249/floridas-new-political-ad-law-could-drive-dollars-state-candidates-online.

[40] National Science Foundation, "A Brief History of NSF and the Internet," http://www.nsf.gov/news/news_summ.jsp?cntn_id=103050; *see also* Barry M. Leiner, Vinton G. Cerf, David D. Clark, Robert E. Kahn, Leonard Kleinrock, Daniel C. Lynch, Jon Postel, Larry G. Roberts, Stephen Wolff, "A Brief History of the Internet," Internet Society (ISOC), http://www.isoc.org/internet/history/brief.shtml.

[41] *Id.*

[42] Jack Goldsmith and Tim Wu, WHO CONTROLS THE INTERNET, 2008.

[43] EPIC, Cybersecurity and Privacy, http://epic.org/privacy/cybersecurity/default.html.

websites might create positives as well as negatives for the free flow of and access to political speech.[44]

As the Internet will probably continue to grow in a largely unsupervised fashion in the near future, users may not be able to rely solely on the strict enforcement of state and federal laws to combat deceptive campaign practices on the Internet. Voters, Election Protection efforts, poll workers, and Election Administrators working together can secure elections against these threats until business practices and government oversight functions evolve to meet the challenges of Internet communications. There are practices that election officials, Election Protection efforts, and voters can employ to greatly reduce the chances that they will become victims of deceptive campaign practices that use the Internet. The good news is that, since 2008, several states have taken steps to regulate potentially deceptive online political campaign messages.[45]

Deceptive campaign practices are based on fraud techniques that are well known in the Internet communication environment. The following terms are familiar to computer security and law enforcement experts and will be used to explain the potential for e-deceptive campaign threats to the 2010 general election. In the context of deceptive election practices, "spoofing," "phishing," "pharming," "denial of service," " rumor mongering," and "social engineering" are tactics that can be used to deceive voters and impact voter participation, as illustrated here.

- **Spoofing** occurs when a website falsely claims to be another, often official, site.[46] For example, a deceptive site claiming to be the State's Election Office might go so far as to appropriate the State's official insignia or seal, but in fact have nothing to do with any official state governmental office. The content of the Web page might provide deceptive information to voters on polling locations, voter registration rules, or polling dates and times.

- **Phishing** is sending fake email to voters offering assistance with locating polling sites, voter record change of address requests, new voters' registration services, or verification of voter registration status.[47] Phishing then asks the email recipient to respond, perhaps by clicking a link, thereby exposing the recipient's computer and computer network to malware.

- **Pharming** is a version of phishing, involving the fraudulent use of legitimate domain names. Pharming attacks can successfully hijack Get Out the Vote (GOTV), election

---

[44] EPIC, Cybersecurity Policy Working Group, Statement on National Strategy for Trusted Identities in Cyberspece, September 2010, http://privacy.org/privacy_coalition_comments_trusted_ids.pdf.
[45] National Conference of State Legislatures, Internet Campaigns, http://www.ncsl.org/default.aspx?tabid=21244.
[46] "Website Spoofing," Wikipedia, http://en.wikipedia.org/wiki/Website_spoofing.
[47] Congressional Research Services, REPORT TO CONGRESS, INTERNET PRIVACY AN OVERVIEW OF PENDING LEGISLATION, 18-19, October 19, 2005, *available at* http://digital.library.unt.edu/govdocs/crs/data/2005/upl-meta-crs-7879/RL31408_2005Oct19.pdf; *see also* United States Computer Emergency Readiness Team (US-CERT), "Avoid Social Engineering and Phishing Attacks," http://www.us-cert.gov/cas/tips/ST04-014.html.

administration, and Election Protection Web addresses and redirect visitors to imposter websites. This approach can also be used to change a voter's computer configuration so that typing a legitimate address will take the user to a fake website.[48]

- **Denial of service** attacks can make voter information sites, GOTV efforts, or voter help hotlines unavailable by clogging up traffic to the website, thereby overburdening the site's servers and causing the site to shut down.[49] For example, by directing voters by the tens of thousands to erroneously contact local election administrators for non-existent voter services such as activating voter registration cards, or known services such as verifying registration status, legitimate sites can crash, leaving voters without access to a critical resource on Election Day.

- **Rumor-mongering** can involve planting stories that sweep through blogs and into the mainstream media, causing confusion amongst the electorate. For example, rumors that the election has been cancelled or delayed by a week due to an emergency might keep voters from the polls.

- **Social engineering** involves tricking people, through non-technological means, into breaking their normal technology security practices; exploiting individuals who are not technologically savvy into exposing important personally identifiable information; or determining the emotional state of an identifiable block of voter to design messages to discourage participation.[50] In the 2010 election season, social engineering for deceptive campaign purposes could include knowing a particular issue that a voter might be sensitive about and exploiting that knowledge. For example, excessive negative messages directed toward voters disenchanted with the progress of a particular program or favored government project could be deployed to discourage those voters' participation in an election.

The strategies for electronic deceptive campaign practices and how they may be deployed to impede voter participation are key components of this report. The recommendations provided after each section are intended to set forth practical steps that voters, Election Protection efforts, Election Administrators, and GOTV projects can consider as they prepare for a successful election experience.

---

[48] *See* Jason Milletary, "Technical Trends in Phishing Attacks," United States Computer Emergency Readiness Team, http://www.us-cert.gov/reading_room/phishing_trends0511.pdf.
[49] United States Computer Emergency Readiness Team (US-CERT), "Understanding Denial-of-Service Attacks," http://www.us-cert.gov/cas/tips/ST04-015.html.
[50] Social Engineering (definition), http://searchsecurity.techtarget.com/sDefinition/0,,sid14_gci531120,00.html; *see also* United States Computer Emergency Readiness Team (US-CERT), "Avoid Social Engineering and Phishing Attacks," http://www.us-cert.gov/cas/tips/ST04-014.html.

Reaching Voters in 2010

The Internet is an invaluable tool for promoting civic engagement and mobilizing voters. The Internet is global and it is not policed or owned by any single entity,[51] providing opportunities for communities to develop outside of geographic limitations and to keep abreast of new political developments.[52] A Pew Research Center report found that 24% of Americans routinely use the Internet to keep information about the election.[53]

Further, Internet communications[54] are not confined to computers. Web communications now also include mobile phones, smart phones (iPhones and Android phones), personal digital assistants (Blackberrys), smart devices (iPad, e-book readers), interactive television systems (TIVO), voice response systems, kiosks, and new applications for consumer appliances. The Pew Research Center has found that 74% of American adults use the Internet, [55] and that 83% of adults have cell phones or smart phones.[56] Political messaging can include Voice over Internet Protocol (VoIP), e-mail, instant messaging, texting, tweeting, mobile ads, Web pages, and blogs. The remainder of this report explores some of these forms of communication and their potential risks for use in e-deceptive campaign attacks.

E-Deceptive Campaigns: Problems and Strategies

Search Engine Requests

Search engines are a critical utility for Internet users.[57] But there is a risk that, as an important election cycle approaches, third parties may seek to provide misleading information to Internet users in an attempt to misdirect voters through search engine results. Search request that have

---

[51] Misha Glenny, "Who Controls the Internet," *Financial Times*, October 8, 2010, http://www.ft.com/cms/s/2/3e52897c-d0ee-11df-a426-00144feabdc0.html.

[52] Federal Election Commission, Internet Communications, Volume 71 Number 70, April 12, 2006 http://edocket.access.gpo.gov/2006/06-3190.htm

[53] Pew Research Center for The People & The Press, SOCIAL NETWORKING AND ONLINE VIDEOS TAKE OFF: INTERNET'S BROADER ROLE IN CAMPAIGN 2008, January 11, 2008, *available at* http://www.pewinternet.org/Reports/2008/The-Internet-Gains-in-Politics/Summary-of-Findings.aspx.

[54]There are basic rules for obtaining Internet or IP addresses, the essential components of online communications. For general information see Internet Corporation for Assigned Names and Numbers (ICANN), http://www.icann.org/.

[55] Pew Internet and American Life Project, THE INTERNET'S ROLE IN CAMPAIGN 2008, available at http://www.pewinternet.org/Reports/2009/6--The-Internets-Role-in-Campaign-2008.aspx, April 15, 2009.

[56] Lee Rainie, Pew Internet and American Life Project, INTERNET BROADBAND AND CELL PHONE STATISTICS, January 5, 2010. http://www.pewinternet.org/Reports/2010/Internet-broadband-and-cell-phone-statistics.aspx

[57] "Web Search Engine," Wikipedia, http://en.wikipedia.org/wiki/Web_search_engine.

typo errors or faulty logic statements may yield results that look like what was requested, but in fact are web pages intended to deceive voters.

Deception in Internet communications is much easier than in physical space because digital theft or misappropriation of graphics, text, and state insignias are much easier to accomplish and may be harder for infrequent visitors to identify as being impersonations of legitimate sites.

Most personal computer users employ Web browser applications (Internet Explorer, Bing, Google Chrome, Safari, Opera or Firefox) to assist with accessing Internet search engine service providers (Google.com, AOL.com, Yahoo.com, Ixquick.com). What may not be well known is that search terms entered into search engines can reveal a great deal about the user, such as medical issues, associations, religious beliefs, political preferences, sexual orientation, financial, and demographic information. In 2005, more than 60 million American adults used search engines on a typical day.[58]

The Internet search engine service providers with abundant resources offer services that present other opportunities to collect data on individual users:

- Google Desktop creates an index of the user's computer files, e-mails, music, photos, chat, and Web browser history;
- MSN Messenger, AIM, Yahoo, ICQ, Trillian, Skype, and Google Talk support instant-message chats between users;
- MSN Maps Live.com, Map Quest, and Google Maps manage information requests on physical addresses, which often include a user's home address;
- Yahoo Mail, MSN Mail, AOL Mail, and Google Mail (Gmail) manage Internet users' e-mail — e-mail may be stored for an indefinite period of time, although some service providers establish self imposed limits on data retention;
- Google and Yahoo Calendars provide users with tools for managing personal and professional schedules;
- Google Earth and Wikimapia provide destination or geography information services that allow users to create content regarding locations or addresses;
- MySpace, Facebook, Twitter, LinkedIn, and Google Orkut provide social networking tools that store personal information such as name, location, and relationship status; and,
- Google Video/YouTube collects information by IP address on the videos watched by users.

[58] Pew Internet and American Life Project, BIG JUMP IN SEARCH ENGINE USE, Nov. 20, 2005, available at http://www.pewinternet.org/Reports/2005/Big-jump-in-search-engine-use/Data-Memo/Findings.aspx, November 20, 2005.

These services collect information on users that can be used to create very detailed profiles. Coupled with search engine results, the majority of routine Internet users are adding current information such as lifestyle, political views, topics, or subjects of interests to the wealth of data collected by third parties.

Search Engine Requests Deceptive Strategies

Can effective deceptive campaign **spoofing** attacks be deployed through user search engine requests?
Yes. *When computer users make search engine requests through Web service applications like google.com, AOL.com, Yahoo.com, and Ixquick.com, the search engine may return a list of spoofed website results that redirects users to fake websites.* *For example, search engine requests seeking information on "Florida polling locations" could return a fake site that resembles the official version of the Florida Division of Election's office website or Election Protection information service providers.* *Requesters may also be misled when searches on Google Maps or Wikimapia have false locations identified as legitimate polling locations.*

Can deceptive campaign **phishing or pharming** attacks be deployed through user search engine requests?
Yes. *This is possible. If someone purchased an ad with the intent to collect information, this ad could be used later to send a deceptive e-mail, text message, etc.* *For example, someone might purchase an Internet Ad that will appear at the top of search results for "Where do I vote Los Angeles?" The ad might link to a page that asks for residential information and e-mail addresses to send a reminder on Election Day to vote. The correct information may appear on the page at the time of the initial request, but the e-mail or text reminder may give the wrong address the evening before or the morning of Election Day.*

Can effective deceptive campaign **denial of service** attacks be deployed in conjunction with search engine requests?
Yes. *Denial of service means that demands to view a page exceed the ability of the Web page host to provide access to*

requesters.

A denial of service attack involves creating an overwhelming number of requests for a single Web page. Once the ability of the Web page hosting service to respond to a page request is exceeded, any other request will not be honored.

This is similar to what happens when a telephone does not have call waiting. The person calling and making a connection can prevent any other calls from successfully connecting.

Because the widespread use of broadband allows for 24-7 computer online connections, there are methods for gaining control of private distributed personal computing resources.

An attacker can deploy the stolen computing resources of many personal computers without the consent of the owners to launch this type of attack.

Can effective deceptive campaign **rumor-mongering** attacks be deployed using search engine requests? **Yes**.

Yes. *Search engine function is in part based on the meta tag– the header information that is part of each Web page.*

Web content creators use meta tag information, among other things, to describe the type of information found on a page.

Web search engine service providers also use meta tag information to help them determine how their search engines will rank the page.

By manipulating meta-tag information, deceptive campaigners may fool requesters into thinking that a deceptive site is the most relevant and accurate site if it is amongst the top results returned.

Can effective deceptive campaign **social engineering** attacks use Web search engine requests to misdirect voters?

Yes. *Search results can provide information on candidate preference, issues of interest, residential neighborhood, social, or cultural interests to social engineers who might then develop Web content that increases the likelihood that certain voters will select links taking them to deceptive campaign information.*

Search Engine Requests Recommendations

- Internet Search Engine Providers (ISPs) should consider if manipulation of the search request environment by those seeking to deploy a deceptive campaign is potentially a problem.

- Web page creators should verify the rankings of election related online election services pages on google.com, AOL.com, Yahoo.com, Bing, Firefox, Ixquick.com and other search engines. Web rankings can be determined based on a number of factors. However, if there are questions about rankings of an organization or entity's Web page, the Web page manager can review information provided online and follow up with search engine service providers.

- Election Administrators and Election Protection should:

    - Review the rankings of official websites to be sure they are at the top of the rankings for the topics sought.

    - Through the media, communicate to voters the URLs (Web addresses) for information on the November 2, 2010 election.

    - Develop plans to address potential problems with Web content pages.

- Individual users should:[59]

    - Verify the correct spelling for search requests or individual URLs.

    - Be sure that requests begin with the most significant and end with the least significant search terms.

    - Use Boolean searches, such as AND, OR, or NOT to search terms, to narrow the search.

    - Adjust search results to raise the probability that the page rank will be most to least responsive, and

    - Contact Election Assistance Programs
        - 1-866-OUR-VOTE or visiting http://www.866ourvote.org/,
        - The National Association of Secretaries of State at http://canivote.org,
        - The National Association for Latino Elected Officials at http://www.yaeshora.info/, or

[59] The Spider Apprentice, How to Use Search Engines, http://www.monash.com/spidap4.html#keyword.

- The Election Administration Commission at http://www.eac.gov/voter_resources/contact_your_state.aspx for election related information on voter registration status, polling location, voter identification requirements, your rights as a voter, and hours of polling operations.

Search Engine Results

New technology may bring deceptive practices on-line by exploiting the way individuals look for election related information. Users' search requests can be linked to their personally identifiable Internet Protocol (IP) address, a unique string of numbers that identifies each individual computer connected to the Internet. Search histories can reveal preferences and political interests. The search results users see include more than just responses to their search query. Internet search engine service providers also rely on their proprietary analysis and consideration of advertising dollars to determine pages relevant to a search.[60] Web advertisements often appear as the first selections on a search results page. Online advertising is not regulated.[61]

When users submit search engine requests, service providers may automatically log and retain information about the user's request, IP address, browser type, browser language, the date and time of the request. One or more tracking "cookies" (small pieces of code) may be installed and stored on the requester's computer to uniquely identify the user by a host website. Cookies also include dates for how long they should be retained, which can be a few days, weeks, months, or years. Tracking may also involve monitoring the activity of visitors once they leave Web pages that deploy cookies.[62] The cookies used by political websites, blogs, or Web videos, could be used to target computers hosting the cookies associated with specific Web activity.

When cookies are retained on users' computers, the computers become vulnerable to spy ware found on websites or hidden in e-mail attachments, video, or audio files. Malware or malicious software can alter stored Web address history data by replacing it with incorrect information.[63]

Another approach to deceptive tactics, especially for campaigns lacking resources, is to manipulate results so that the campaign's pages rank higher than the sought page. This is

---

[60] "Web Search Engine," Wikipedia, http://en.wikipedia.org/wiki/Web_search_engine.
[61] Grant Gross, "FTC Sticks with online advertising self-regulation," *Network World*, February 12, 2009, http://www.networkworld.com/news/2009/021209-ftc-sticks-with-online-advertising.html.
[62] Tanzina Vega, "New Web Code Draws Concern over Risks to Privacy," *The New York Times*, October 11, 2010, *available at* http://www.nytimes.com/2010/10/11/business/media/11privacy.html?_r=1&hp.
[63] EPIC, E-DECEPTIVE CAMPAIGN PRACTICES REPORT: INTERNET TECHNOLOGY & DEMOCRACY 2.0, Appendix A, October 2010.

especially true with sponsor Ad-based page search results if an opponent purchases all of the ad words associated with a campaign effort and redirects requests to pages. Often web browser users will not look beyond the first or second page of search results if they do not see the information they are seeking. Any effort to lower the page rankings of legitimate pages with election related information would be a deceptive attack.

Search Engine Results Deceptive Strategies

Can effective deceptive campaign **spoofing** attacks be deployed with search engine results?
Yes. *Web search engine results are based on search terms provided by users.* *But an attack might spoof websites requesters are searching for– the false site may appear in every way to be the website the user expects to see, but might, in fact, provide false information.* *For example, a search for "Nevada polling locations" could return a list of results that may spoof the Web identity of the state's top election administrator's website or Election Protection information service providers.*

Can effective deceptive campaign e-mail **phishing or pharming** attacks be deployed in conjunction with search engine results?
Yes. *This type of attack could involve accessing the browser history of Internet users to change stored information such as bookmarked e-addresses, cache memory, or the users "host file."* *The host file is a directory of Internet addresses that can be edited to direct user Internet address requests to fake sites.*

Can effective **denial of service** attacks be deployed in conjunction with search engine results?
Yes. *Malicious computer software may be used to infect computing systems by directing that infected computers send multiple ping requests to a target computer system at a set time and day.* *Selecting a link to a deceptive site can expose a personal computer, laptop, personal digital device or Web enabled cell phone to damaging software invasions in the form of viruses, worms, or Trojan horses designed to carryout a denial of service attack.*

The same threat exists when downloading video clips, photos, music, or other media based files.

Can effective deceptive campaign Internet **rumor-mongering** be deployed using search engine results?

Yes. *Search engine results are based in part on the meta tag, header information that is part of each Web page.*

Search engines use software to read meta data to sort and manage pages sought by users. Meta tag data provides identification information to search engines as to what can be found on the hosted page.

For example, meta data identification could state that the Web page contains information on "polling location, Pennsylvania, Michigan, Virginia," but in fact not provide that information.

Further, this same meta tag data could be used to avoid the intended purpose of the user's search request.

For example, meta tag information might use "polling location," "election day assistance," "voter registration," "Virginia," "Pennsylvania," or "Florida," while the content of the pages could in fact provide rumor-mongering fodder such as "terrorism plot on Election Day," or "Emergency polling location relocation plan," or "New polling location hours due to flooding at polling locations." Each of the results may sound plausible but each would be false.

Can effective deceptive campaign **social engineering** be deployed using Web search engine results?

Yes. *Search results that indicate a preference for a particular candidate or issues that indicate ideological beliefs, or residential neighborhoods can provide information to social engineers. Social engineers could then develop Web link information that increases the likelihood that certain voters will select links taking them to deceptive campaign information.*

Search Engine Results Recommendations

- Search engine providers should be alert to the possibility of new Web content pages that attempt to deploy deceptive campaign information about the November 2, 2010 election.

- Election Administrators and Election Protection should:

    - Know how to contact the top ranked Internet Search Engine Providers Google.com, Bing, Yahoo.com, Ixquick.com in the event of an emergency.

    - Create contingency plans to address problems around presentation or access to Web pages.

- Internet users should:

    - Contact Election Assistance Programs
        - 1-866-OUR-VOTE or visiting http://www.866ourvote.org/,
        - The National Association of Secretaries of State at http://canivote.org,
        - The National Association for Latino Elected Officials at http://www.yaeshora.info/, or
        - The Election Administration Commission at http://www.eac.gov/voter_resources/contact_your_state.aspx for election related information on voter registration status, polling location, voter identification requirements, your rights as a voter, and hours of polling operations.

    - Know that the date of all National Elections is set by Federal law to be the first Tuesday after the first Monday in November, which in 2010 is November 2.

    - Check for software updates for their personal computer's operating system, like Windows, Macintosh, or Linux.

    - Consider alternatives for Web page browser and e-mail application: see http://epic.org/privacy/tools.html.

    - Verify the correct spelling for search requests.

    - Know that the first few search results will typically be for advertisements.

    - Begin with the most significant and end with the least significant search terms.

- Use, if possible, Boolean searches by including AND, OR, or NOT in the search term, to narrow the search,[64] and,

- Adjust search results to raise the probability that the page rank will be most to least responsive.

Social Networking Sites

Social networking sites, such as MySpace, Facebook, and BlackPlanet have become established forums for keeping in contact with old acquaintances and meeting new ones.[65] Users can create their own Web page and post details about themselves, such as where they went to school, their favorite movie titles, and their relationship status. They can also exchange messages and share information and photos with friends. Many people in their teens and 20s use social network sites rather than email for the bulk of their online communications. Social networking sites also play a significant role in younger activists' political participation.[66]

These sites allow millions of users to identify their causes and affiliations. Savvy organizers make use of this largely public information to reach out to individuals to build coalitions and networks.[67] In 2008, many of the over 750,000 people who participated in the "One Million Strong for Barack Obama" Facebook group had previously been active in "get out the vote" and "know your rights" work, phone banking, fundraising, and other activities.[68]

A *Wall Street Journal* investigation revealed that third-party applications provided to Facebook users for entertainment or information services are also sharing personal information on users with marketers.[69] The data collected could be used in ways that are not in the interest of consumers or voters.

For example, one approach to e-deceptive practices on social networks would be for a group of attackers to infiltrate a large social networking group to share misinformation about the November 2, 2010 election. The first step would be to identify like-minded users, a relatively

---

[64] The Spider Apprentice, How to Use Search Engines, *available at* http://www.monash.com/spidap4.html#keyword.

[65] "2010 Social Networking Websites Review Comparison," toptenreviews.com, http://social-networking-websites-review.toptenreviews.com/.

[66] *See* Morley Winograd and Michael D. Hais, MILLENNIAL MAKEOVER: MYSPACE, YOUTUBE, AND THE FUTURE OF AMERICAN POLITICS (2008); website at http://www.millennialmakeover.com/.

[67] *See* Sean Spence, "Local political campaigns using social networking," *Columbia Business Review*, February 5, 2010, http://www.columbiabusinesstimes.com/7055/2010/02/05/local-political-campaigns-using-social-networking/.

[68] *See* postings on Jon Pincus's blog, *Liminal States*, Cognitive Diversity in the 2008 US election, March 2008, *available at* http://www.talesfromthe.net/jon/?p=111and A One Million Strong Facebook moneybomb!, October 2008, *available at* http://www.talesfromthe.net/jon/?p=231.

[69] Austin Business Journal, Report: Facebook app IDs invade privacy, October 18, 2010, http://www.bizjournals.com/austin/news/2010/10/18/report-facebook-app-ids-invade-privacy.html

easy task. Sites like Facebook and MySpace allow the general public to search their databases of members through search terms such as a name, e-mail address, or school. In many cases, information can also be filtered by country, state, and even to a postal code. If users adjust their privacy settings to allow viewing of their full profiles, search results will provide additional information such as occupation, hometown, sexual orientation, ethnicity, and religion.

The attackers could spread false information in several ways. For example, one member could post some deceptive information on the group's discussion board, with a link to a site that claims to corroborate it. If several other attackers quickly confirm the false information and nobody takes the time to debunk and counter it with facts, at least some group members may regard the deceptive information as the truth.

Other approaches to using groups for deception are possible as well. For example, partisan political operatives could infiltrate a group or friend key influencers to gain trust, later using their relationship to sow mistrust about particular candidates. Operatives could also set up a group that initially provides accurate information and projects a political perspective that appeals to targets. The group could then cultivate and encourage greater participation based on its content. The deceptive campaign could be launched a day before the election by posting a message that is false or misleading to participants who may act on it, having previously found the group to be reliable.

Social networking sites are also ideal for viral message spread. For example, by putting deceptive information on a user's profile, the potential to deceive not only the user being directly targeted, but also all of his friends who will see the information on his profile or newsfeed, rises exponentially. Online "friend" relationships may be based solely on limited remote communication. The level of trustworthiness placed in the information shared among friends can be exploited to spread misinformation. A social networking campaign combined with a traditional e-mail deception tactics could reinforce false information from what appear to be independent sources.

Another feature of Social Networking that may be exploited is the use of "Like" buttons as a way of supporting a page or its content, through something called "likejacking."

The larger challenge for social networking users is navigating the volume of anonymously funded political advertising and speech during this election cycle.[70] Because people who are using social networking sites are often sophisticated and well educated, the tactics deployed will be more subtle and nuanced. The tactics often rely on manipulating the emotional and mental states of voters, which are powerful tools for suppression campaigns. Users should research the political commentary they are encountering in these environments.

[70] Editorial, "What the Anonymous Campaign Donors Want," *The MetroWest Daily News*, October 18, 2010, http://www.enterprisenews.com/news/news_columnists/x1404221108/Editorial-What-the-anonymous-campaign-donors-want.

More positively, social network sites also have the ability to counter deceptive practices by getting the word out. In 2008, the Obama campaign released a "debunking the myths" video on YouTube, making it easy for supporters to get the word out online.[71] The rapid information-sharing and discussion typical in these environments can expose deceptions and spread the facts instead of the falsehoods. Grassroots election protection campaigns such as the Twitter Vote Report and Voter Suppression Wiki are using social networking to engage large numbers of activists to fight deceptive campaign practices.[72]

Social Networking Sites Deceptive Strategies

Can effective deceptive campaign **spoofing** attacks be deployed through Social network sites?
Yes. *Social networking sites promote participant hosting of interest groups and events to engage and inform users on a wide range of topics.* *For example, a group like "Progressives for Change" or "Tea Party All the Way" could issue invitations based on registered user profiles. These groups could then disseminate false information about the candidates and their stance on issues.* *Another example is "likejacking," or a "clickjack" attack that indicates that a page is one that a Facebook user "likes." These "likes" show up in Facebook users' profiles, which are picked up by "friends." If selected by a Facebook friend the cycle starts anew.*[73] *Social network sites also allow the creation of user tools, applications, and advertisements that can attract users to participating in groups.*

Can effective deceptive campaign e-mail **phishing or pharming** be used in conjunction with social network sites?
Yes. *Social network sites can be created using graphics that may give the impression that the page is hosted by a trusted*

[71] Organizing for America, "Community Blog Obama Myths Debunked," October 25, 2010, http://my.barackobama.com/page/community/post/nywoman/gG5BNM.

[72] Social networking services are free speech zones that use the best features of the Internet to share ideas and encourage broad participation among diverse users. For more information on this topic, see Common Cause, The Lawyers Committee for Civil Rights Under Law and the Century Foundation, **DECEPTIVE PRACTICES 2.0: LEGAL AND POLICY RESPONSES**, October 2008.

[73] Sarah Perez, "Likejacking" Taking Off on Facebook, available at http://www.readwriteweb.com/archives/likejacking_takes_off_on_facebook.php, June 1, 2010

party or entity. *For example, a social networking page might, unlawfully, use an official governmental seal on their site and then provide voters with wrong or incomplete information.*

Can effective deceptive campaign **denial of service** attacks be deployed against or by using social network sites?
Yes. *The threat comes from the potential for a campaign orchestrated on a social network site to launch a denial of service against some other site.*

Can effective deceptive campaign Internet **rumor-mongering** be deployed using social network sites?
Yes. *Social networking sites would be fertile ground for encouraging deceptive campaign rumor-mongering.* *For example, attackers could design a message to turn off voters to the election, or spread misinformation about the right to participate through spreading false rumors.* *Fact checking services are not part of the social networking experience.*

Can effective deceptive campaign **social engineering** attacks use social network sites?
Yes. *Social network sites can promote the targeting of voters who are supportive of a particular candidate or issues.* *Social engineering may be a particularly effective deceptive campaign strategy because of the amount of personal information provided by users.*

Social Networking Sites Recommendations

- Election Protection and Election Administrators should:
    - Create Facebook, Myspace, BlackPlanet, Mi Gente, Twitter, and Friendster pages to reach voters, and publicize the links on their home page.

  - Verify social network accounts when possible (Twitter provides this service.[74]

- Administrators and members of large groups on social network sites should be on the lookout for deceptive information, collaborate with a legitimate source of voter information (such as Election Administrators and Election Protection), and support efforts to swiftly move to counter deceptions related to voter participation rules.

- Visitors to a social network page or group that claims to be associated with an election protection organization should double-check that organization's Web page to ensure that it's not a spoofed site.

- Users of social network sites who are interested in combating deceptive campaign practices should get involved with one of the many social network-based grassroots election protection initiatives.

- Users of social network sites should:

  - Take steps to protect their privacy by learning more about the privacy policy of the service.

  - Change default privacy settings to higher privacy settings to gain more control over their information.

VoIP or Voice over Internet Protocol

VoIP is Internet based telephony supported by hardware and software. VoIP Internet telephony services can be part of a Web browser program or a stand-alone Web product. Internet telephone services can send to or receive calls from traditional telephone services. VoIP service only requires a broadband or high speed Internet service connection and a modem usually provided by the service provider. Recipients of VoIP calls do not need to have either special equipment or high-speed Internet service.[75]

VoIP Political Robocalls

Routinely, political campaigns use telephone banks or call centers to communicate fundraising and other political messages to voters.[76] VoIP can be deployed to deliver similar political telephone messaging from any location in the world at a fraction of the cost. The added

---

[74] Twitter, About Verified Accounts, available at http://support.twitter.com/groups/31-twitter-basics/topics/111-features/articles/119135-about-verified-accounts

[75] Federal Communications Commission, VoIP Frequently Asked Questions, *available at* http://www.fcc.gov/voip/; *see also* Matthew DeSantis, Understanding Voice over Internet Protocol (VoIP), United States Computer Emergency Readiness Team, http://www.us-cert.gov/reading_room/understanding_voip.pdf.

[76] *Id.*

challenge of VoIP in the area of e-deceptive campaign practices is that the technology will not reliably tie the communication to any particular entity or geographic location. Caller ID services that identify the source of telephone calls can have little effect in identifying the location of a call.[77]

For example, Instant Call Blaster is a commercial robo VoIP based call service. The company claims that the service can be established through an Internet application process that can be completed in minutes. Users can begin making calls within seconds. The company has a service that targets political campaign messages called "Political Blast." The company provides a "user friendly web based platform to upload lists, record calls, and launch them with a click of a mouse." [78] Prospective clients are told "if you set up an account with us, you will have access to make calls after business hours and on weekends. This is a bonus for anyone that has an emergency notification, a last-minute political message, appointment reminder, change in venue for a concert, a rain delay or schedule change for tomorrow's game, or to mobilize workers for a strike." [79]

The Federal Election Commission (FEC) currently regulates campaign telephone banks by stipulating that they must contain disclaimers clearly stating whether a committee paid for the communication.[80] In 2006, the FEC implemented regulations based on the court decision *Shays v. Federal Election Commission*.[81] The FEC regulatory authority now "includes paid Internet advertising placed on another person's website, but does not encompass any other form of Internet communication."[82]

E-deceptive campaign messages using VoIP telephony could be accomplished in a several ways. For example, a call that appears on the caller ID as originating from a legitimate election administration authority could inform voters that their poll location has changed and provide incorrect information. A VoIP message regarding voter registration can be effective in misdirecting voters about their registration status. A VoIP deceptive campaign message could target poll workers with a telephone message the evening before or the morning of an election that sends them to the wrong polling location.

---

[77] *Id.*
[78] InstallCallBlast.net, http://instantcallblast.net/servicespolitical.php.
[79] *Id.*
[80] *See* Federal Election Commission, Title 11, Chapter 1, Section 100.28 Scope and Definitions, Telephone Bank, (2 U.S.C. 431(24)), *available at* http://edocket.access.gpo.gov/cfr_2008/janqtr/11cfr100.28.htm and Federal Election, Title 1, Section 100.17, Scope and Definitions, Clearly Identified (2U.S.C. 431(18)), *available at* http://edocket.access.gpo.gov/cfr_2008/janqtr/11cfr100.17.htm.

[81] Shays v. Federal Election Commission, 337 F. Supp. 2d 28 (D.D.C. 2004), aff'd, 414 F.3d 76 (D.C. Cir. 2005).
[82] Federal Register Notice, Federal Election Commission, Volume 70 Number 71, April 12, 2006, available at http://edocket.access.gpo.gov/2006/06-3190.htm.

VoIP Deceptive Strategies

Can effective deceptive campaign **spoofing** attacks be deployed using VoIP Internet telephony?
Yes. *VoIP can be an effective tool in a deceptive campaign attack. Calls do not need to originate in the United States. A caller ID system cannot identify the call's origination point.* *Because the calls can be completely automated (i.e. a taped message) or caller operator supported, they are difficult to trace. The message could provide inaccurate caller ID information to add to the complication of tracing the source of the call.* *The message can incorrectly identify the source of the call and the message can relay false information such as erroneously telling voters their polling location has changed.*

Can effective deceptive campaign e-mail **phishing or pharming** attacks be deployed in conjunction with VoIP Internet telephony?
Yes. *Phishing attacks could suggest that you call a certain phone number to contribute to your favorite candidate.* *For example, one phishing attack in 2008 told voters they must call to verify their registration 24 or 48 hours before the election. At this point, the voter registration offices are at their busiest and cannot deal with mass calls about registration or polling locations. It would be in effect a denial of service attack that voters would launch against their own election administration offices.*

Can effective deceptive campaign **denial of service** attacks be deployed in conjunction with VoIP Internet telephony?
Yes. *A denial of service attack launched against a Get Out the Vote (GOTV) effort in New Hampshire in 2004 was identified because the calling operation used traditional domestic telecommunication services. The attack was effective in jamming the incoming call lines to local fire station providing voters with free rides to the polls.*[83]

[83] John DiStaso, Dems, "GOP settle phone lawsuit," *The Union Leader*, A1, December 2, 2006, *available at* http://bit.ly/9rCbRL.

Similarly, a VoIP attack's goal could be to occupy every available phone number so that legitimate calls cannot get through. A VoIP deceptive campaign attack could make it nearly impossible to reach an Election Administrator's office, Election Protection information line, GOTV assistance service provider, or campaign office for assistance during the critical hours of an election.

Can effective deceptive campaign Internet **rumor-mongering** attacks be deployed using VoIP Internet telephony?
Yes. *VoIP would be extremely effective in launching deceptive campaign rumors because of its low cost and the near impossibility of tying an entity to the calls made.* *VoIP can be used to start new or spread old rumors like "terrorism plot on Election Day," "Election cancelled due to candidate illness," "If you have unpaid parking tickets you cannot vote," or "Emergency polling location relocation plan."*

Can effective deceptive campaign **social engineering** attacks be deployed using VoIP Internet telephony?
Yes. *Social engineering is effective when an attacker convinces recipients of calls to provide personal information under a false pretext.* *For example, a call message could be "The Election office asked that we contact you because you have not activated your voter registration card for next week's election. Could you tell me your Social Security Number?"* *This type of attack has been used in the past against registered voters.*[84]

VoIP Recommendations

The potential for deceptive VoIP telephone banks is high. Unfortunately the resources of election officials and voter participation advocates to fend off attacks may be limited. The best defense against a VoIP deceptive campaign attack is arming voters with good information on their right to participate in the election.

[84] Benita Y. Williams, "Election officials warn of scam," *The Kansas City Star*, September 29, 2004.

- Election Administrators and Election Protection efforts should:

    - Explore the use of VoIP services on Election Day as emergency backups for traditional telecommunications. Cell phones may provide alternative links to key personnel during critical election periods.

    - Repeat often the dates for early voting and the very important date of the general election — November 2, 2010.

    - Contact Election Assistance Programs
        - 1-866-OUR-VOTE or visiting http://www.866ourvote.org/,
        - The National Association of Secretaries of State at http://canivote.org,
        - The National Association for Latino Elected Officials at http://www.yaeshora.info/, or
        - The Election Administration Commission at http://www.eac.gov/voter_resources/contact_your_state.aspx for election related information on voter registration status, polling location, voter identification requirements, your rights as a voter, and hours of polling operations.

- Internet users should:

    - Vote early if that option is available to them.

    - Contact Election Assistance programs
        - 1-866-OUR-VOTE or visiting http://www.866ourvote.org/,
        - The National Association of Secretaries of State at http://canivote.org,
        - The National Association for Latino Elected Officials at http://www.yaeshora.info/, or
        - The Election Administration Commission at http://www.eac.gov/voter_resources/contact_your_state.aspx for election related information on voter registration status, polling location, voter identification requirements, your rights as a voter, and hours of polling operations.

    - Know that the last day to cast a vote in the General Election is November 2, 2010.

Web Advertising and Behavioral Targeting

Online advertising has emerged as an influential tool for online revenue generation for Internet Service Providers (ISPs). "Micro-targeting" encompasses all of the activity that is employed by ISPs and advertisers to monitor Internet users. Most Internet consumers are unaware that their

online activity may be monitored for the express purpose of targeting advertisements or building user profiles.[85]

A related development has been the use of "black boxes" on ISP networks to monitor user traffic. The actual workings of these black boxes are unknown to the public. What little information has been made public reveals that many of the systems are based on "packet sniffers," typically employed by computer network operators for security and maintenance purposes. These are specialized software programs running in a computer that are hooked into the network at a location where they can monitor traffic flowing in and out of systems. These "sniffers" can monitor the entire data stream by searching for keywords, like "Rand Paul" or "Obama," or phrases or strings, such as net addresses or e-mail accounts. The "sniffers" can then record or retransmit anything that fits its search criteria for further review.[86]

In addition, the header information of IP packets in transit between a requester and an ISP can reveal the source, type, and intended destination of an Internet communication. This information can also be used to manipulate destination and routing of requests sent by Internet users. Further, the Web advertising and Behavioral Targeting techniques can be used to reveal different page views to different page viewers. For example, a viewer identified as a friendly voter could see correct information regarding polling locations and times while a voter indentified as not being friendly could see a page with inaccurate or deceptive information.

DPI can be deployed in an e-deceptive campaign attack. For example, a message that originates or is destined for a Web service sponsored by a campaign, election administrator, or election advocacy organization could be slowed down significantly as it is routed by the user's Internet service provider. Net Neutrality advocates have argued that Deep Packet Inspection permits this type of network discrimination.[87]

Web Advertising and Behavioral Targeting Deceptive Strategies

Can effective deceptive campaign **spoofing** be deployed using Web advertising or behavioral targeting?
Yes. *There is no effective regulation of the type of information that Web page owners might collect from visitors. Web content creators may track visitors to their sites. If they also host ads, the site's visitors may also be tracked by the advertisers.* *Ad space is managed by Internet Service Providers. Ads are*

[85] Center for Digital Democracy, Digital Marketing, Privacy & the Public Interest, *available at* http://www.democraticmedia.org/current_projects/privacy.
[86] EPIC and Privacy International, PRIVACY & HUMAN RIGHTS, 62-63, (2005).
[87] *See for example,* Free Press, *Deep Packet Inspection: The End of the Internet as We Know It?*, March 2009, *available at* http://www.freepress.net/files/Deep_Packet_Inspection_The_End_of_the_Internet_As_We_Know_It.pdf.

typically the first links provided to users seeking information. Election Protection, Election Administrators, and Internet Service Providers should be aware that attempts to spread deceptive information by appropriating the name or Web identity of trusted entities are possible.

Search engine providers do not regulate the content of Web pages that are provided by advertisers. The FEC has also advised that a search engine, like Google, need not disclose who pays for the political advertising it runs as of now. The FEC is continuing to examine this issue.[88]

Can effective deceptive campaign **phishing or pharming** e-mail attacks be used in conjunction with Web advertising and behavioral targeting?
Yes. *Pharming and phishing attacks might use Web advertising and behavioral targeting to develop a list of potential victims.*

Can effective deceptive campaign **denial of service** attacks work using Web page advertisements and behavioral targeting?
No. *This type of deceptive campaign-based attack would not yield as great a result as some of the other strategies presented in this report.*

Can effective deceptive campaign **rumor-mongering** attacks be deployed using Web advertising and behavioral targeting?
Yes. *Web advertising and/or behavioral targeting used in conjunction with an e-mail, social networking, or VoIP attack would pose a serious challenge.* *The more that is known about the personal lives and habits of perspective voters, the greater the likelihood that an attack would be successful.* *The deception could falsely attribute the source of the rumor attack to an innocent candidate or party.*

Can effective deceptive campaign **social engineering** attacks use

[88] Federal Elections Commission, Memorandum, Draft AO 2010-19 (Google) -Revised Draft C, October 7, 2010.

Web advertising and behavioral targeting?
Yes. *Web advertising and behavioral targeting is furthered by the ability of marketers to surreptitiously collect information on the online habits of Internet users.* *For example, a pro-progressive or pro-conservative group could place an ad on a site. The advertiser could monitor users and provide the campaign with the information it gathered.* *With this information, deceptive campaigns could better target messages for intended recipients.*

Web Advertising and Behavioral Targeting Recommendations

- Search engine providers and Web pages that host ads should be aware that election related ads could be a vehicle for hosting deceptive campaign efforts.

- Election administrators and Election Protection efforts should monitor online content for misappropriation of e-logos and content pages.

    - Search Google.com, Yahoo.com, MSN.com, and Ixquick.com, for relevant pages or Web sites hosted by your organization. If problems are identified, contact the search engine provider for more information.

- Individual users should:

    - Know that behavioral targeting is part of their Internet experience.

    - Report suspected deceptive campaign problems related to behavioral targeting and false Web advertising to the Federal Election Commission. http://fec.gov.

    - Consider using personal computing security tools.

    - Learn more about privacy enhancing tools: http://epic.org/privacy/tools.html.

Web Blogs and Web Pages

Blogs are a great resource for political news and commentary. They are a leading source of news and campaign information from millions of voters. The issues outlined in this section are not about the very good work that political blogs are doing, but the need to be aware of the potential for deceptive campaign messages. Corporate political speech is virtually unlimited this election cycle. Corporations, acting alone or in conjunction with others, fund ads and campaigns without limits. When deciding whether to act on a message posted to a blog or

website, voters should consider how much they trust the site by thinking about the longevity of the site and its editorial consistency. Is the site really a grassroots effort or a marketing tool for a message or opinion clothed as a public or community service organization?

Web blogs and Web pages can accomplish more than simply providing information to visitors to their sites. They are also a resource for campaigns to address issues of concern to their supporters, engage the media, and speak directly to voters on critical issues. In 2008, John McCain's campaign established a web site, "John McCain's Truth Squad," to defend his military record.[89] Barack Obama's campaign established a Web page, "Fight the Smears, to correct disinformation and misinformation attacks."[90]

Web blogs and Web pages may also support cookies or flash cookies, which can facilitate the tracking of users while online.[91] Blogs and Web pages can attract visitors through a number of methods such as referral by popular blogs, e-mails citing information found on blogs, or through news reports. Web blogs and Web pages may contain advertising that uses cookies to tag visitors to their sites. They can also deploy malicious software that can do harm to personal computers.[92]

Web Blogs and Web Pages Deceptive Strategies

Can effective deceptive campaign **spoofing** attacks be deployed using Web blogs or Web pages?
Yes. *Third parties may attempt to spoof legitimate political Web blogs and Web pages.* *For example, a search result for a popular political blog might return a website spoofing the requested site. The spoofed site could be an advertisement.* *This could also happen with a Web page hosted by an election administrator or Election Protection effort.*

Can effective deceptive campaign **pharming and phishing** attacks use Web blogs or Web pages?
Yes. *Deceptive phishing campaigns link to fake websites.*

Can effective deceptive campaign **denial of service** attacks be

[89] John McCain for President, Truth Squad, *available at* http://www.johnmccain.com/truthsquad/.
[90] Organizing for America, Fight the Smears, *available at* http://fightthesmears.com/.
[91] EPIC, Flash Cookies, *available at* http://epic.org/privacy/cookies/flash.html.
[92] *Id.; see also,* EPIC, E-DECEPTIVE CAMPAIGN PRACTICES REPORT, Appendix A, October 2010.

deployed in conjunction with Web blogs or Web pages?
Yes. *Though this type of attack would be highly unlikely, there are several approaches that should be considered.* *An attack could be designated to misappropriate a Web blog or Web page address of a recognized trusted source for the purpose of spreading misinformation.* *Web blogs and Web pages authored by new sources could be used to launch deceptive campaign denial of service attacks on phone operations for election officials, Election Protection, or campaigns.*

Can effective deceptive campaign **rumor-mongering** be deployed using Web blogs or Web pages?
Yes. *Web blogs and Web pages have control over page content. The larger threat posed by electronic deceptive campaigns is when unfounded rumors take on the air of authority then spread beyond the limited audience of the Web blog or Web page's readership.*

Can effective deceptive campaign **social engineering** attacks be deployed using Web blogs or pages?
Yes. *Web blogs or Web pages could be used in conjunction with other Internet based communications such as an e-mail or instant messaging to launch deceptive campaigns.* *Social engineering attacks focus on getting the cooperation of the victim to do something for the attacker.* *By appealing to the hearts rather than the minds of voters, attackers can encourage voters to act on deceptive information*

E-mail and Instant Messaging

National political campaign efforts are relying on instant messaging, e-mail, and Web sites to manage the communication environment. One out of every six Americans has received e-mails from or sent e-mails to family and friends, with 14% of them reporting receiving e-mails

from political groups or organizations regarding the 2008 campaign.[93] Campaigns targeted e-mail users for instant messages related to fundraising and get out the vote efforts. This fast-paced means of reaching constituents may compress the time needed to launch an effective deceptive campaign attack.

Deceptive campaign e-mail attacks may take the traditional form of deceptive campaign tactics by, for example, telling recipients that Democrats vote on November 2, 2010 and Republicans vote on another day. However, the increasing sophistication of these voters will require that an effective attack be creative and well planned. For example, the recipients of a deceptive email may not be the ultimate target. An attacker may send an e-mail that tells the recipient to call the local election administrator's office to verify registration status or confirm a polling location. The deceptive e-mails appearing to come from Election officials could prompt thousands of calls at a time when local election administrators are struggling to open polls and answer legitimate questions from voters.

The more successful deceptive e-mail attack is one that can prompt the assistance of well-intentioned e-mail users to spread a deceptive message. Any e-mails received regarding voter identification requirements, straight party voting rules, or other election advice should be viewed with a grain of salt. For example, an e-mail stating that voter identification may be a problem on Election Day and recommending that voters bring additional identification such as a Social Security card, birth certificate, driver's license, or state ID sounds plausible, but it is in fact a deceptive message. Any e-mail message claiming to have new information applicable to all voters is likely to be false. Rules governing voter participation, including those about voter identification requirements, are state specific.[94]

Another deceptive campaign might direct voters in the marking of their ballots to create some unique feature that identifies it as having been cast by those targeted with the message. Altering a ballot will disqualify it from being counted. For example, targeted voters may be told how to cast a "straight party" ballot for all Republican and Democratic candidates. They may be told erroneously to vote for both Barack Obama and the straight Democrat party selection. The straight party ballot on an e-slate voting system might be cancelled, thus voiding the ballot.[95]

Election Protection provides a reliable source for information on voter identification requirements for each state—1-866-OUR-VOTE or http://www.866ourvote.org/state/.[96] Voters can also get information from the National Association of Secretaries of State at

---

[93] Pew Research Center for The People & The Press, SOCIAL NETWORKING AND ONLINE VIDEOS TAKE OFF: INTERNET'S BROADER ROLE IN CAMPAIGN 2008, 8, January 11, 2008, *available at* http://www.pewinternet.org/Reports/2008/The-Internet-Gains-in-Politics/Summary-of-Findings.aspx.

[94] *See* http://canivote.org/ or http://www.eac.gov/voter_resources/contact_your_state.aspx for information about state specific rules about voter eligibility.

[95] Kelly Shannon, "Democrats cry foul over suspicious e-mail," *Dallas Morning News*, October 15, 2008, http://www.dallasnews.com/sharedcontent/dws/news/politics/national/stories/101508dnpoltxemail.235fdd9.html.

[96] Election Protection, In Your State, *available at* http://www.866ourvote.org/state/.

http://canivote.org, the Election Administration Commission at http://eac.gov, or the National Association of Latino Elected Officials at http://www.yaeshora.info/.

A serious line of attack may target poll workers who are key to the proper conduct of public elections. Messages designed to misdirect poll workers could address their role in opening polling locations, rules regarding voter participation, or the appropriate steps that should be taken when faced with administrative questions during an election.

E-mail worm and virus programs have been on the decline because of better security reaction and response when they are detected. The application of security patches and heightened awareness of e-mail users has diminished the damage caused by bogus e-mail. However, there are e-mail attacks that continue to see a measure of success, and there may be future strategies that would disadvantage e-mail users.

Phishing and Pharming are two successful spoofing attacks routinely used by Internet thieves. By posing as legitimate businesses, Internet thieves acquire sensitive information such as logons and passwords, credit card numbers and PINs (Personal Index Numbers), and electronic bank account information. The thieves then send e-mails to unsuspecting individuals in the hope that they will provide their passwords or other personal information.

Phishing deceptive campaigns can involve "social engineering" tactics that use the victim's cooperation to succeed.[97] The sender of an e-mail may pose as a campaign, news source, or election administrator's office. The e-mail may ask the recipient to select a link included in the message. The section of this report on Web blogs and Web pages outline vulnerabilities related to this type of attack.

Pharming is an attack that redirects legitimate Internet traffic to imposter Web sites. Deceptive campaign attacks employing pharming tactics may manipulate information stored in an Internet user's computer cache or the stored registry of domain name system (DNS) addresses. When users visit a website posing as a legitimate election information resource, malicious software might be installed onto the user's machine without any immediate visible effects.[98]

Malicious software can be designed to access personal e-mail address books or sent e-mail outboxes.[99] The attack might activate the e-mail application and send itself to the last 50 persons e-mailed by the user or those listed in the user's e-address book. One infected machine within a computer network can potentially bring down the e-mail application for an entire organization by starting a repetitive cycle of sending e-mails that infect other personal computers. The cycle of infecting computers in the network will continue without end as the inboxes of organization staff receive these messages. It may be hard to distinguish e-mail messages that are legitimate from those that are a result of malicious software. The disruption

---

[97] Bruce Schneier, Cyrpto-Gram, October 15, 2005, *available at* http://www.schneier.com/crypto-gram-0510.html#1.

[98] EPIC, E-DECEPTIVE CAMPAIGN PRACTICES REPORT: INTERNET TECHNOLOGY & DEMOCRACY 2.0, October 20, 2010, Appendix A.

[99] *Id.*

of the e-mail system will continue until computers are made immune to the malicious code and it is removed from every infected computer.[100] This type of attack can be disastrous for an Election Protection or Election Administration operation in the midst of an Election Day.

E-mail and Instant Messaging Deceptive Strategies

Can successful deceptive campaign **spoofing** attacks be deployed using e-mail and instant messaging?
Yes. *E-mail and instant messaging spoofing can be used by deceptive campaigns to suppress voter participation.* *For example, an election deceptive campaign might e-mail or instant message to voters that those in Indiana must activate their voter registration by clicking the link in the email in order to vote on Tuesday, November 2, 2010. This might seem plausible, but it would be a deceptive communication.*

Can successful deceptive campaign **pharming and phishing** attacks use e-mail and instant messaging?
Yes. *Both tactics can be deployed to deceive voters and misdirect those seeking election related information from a trusted source.* *E-mail and instant messaging users may share their addresses voluntarily or have that information collected without their knowledge by Web sites.* *In addition, e-mail and instant messaging addresses may be collected in off-line exchanges such as contests, applications, or other commercial activities.* *Many Internet e-mail users apply filters to avoid SPAM and other unwanted communications, but the user must previously identify the source of the communication as objectionable.* *The ease of creating e-mail addresses, coupled with creative "subject" header descriptions, may increase the likelihood that a recipient will open a deceptive e-mail.* *Further, e-mails can be designed to report back to the source of the communication when a message is opened, especially if the user's computer settings allow embedded images to be*

[100] *Id.*

automatically downloaded.

Can successful deceptive campaign **denial of service** attacks be deployed in conjunction with e-mail and instant messaging?

Yes. *This type of attack would be highly likely for deployment as an electronic deceptive campaign attack.*

Denial of service attacks can be launched from any where in the world. Tese attacks have been launched from Eastern Europe, Pakistan, China, and Russia. Botnets are the tool of choice for online denial of service attacks.[101]

Botnets or bots are automated software designed to maximize the effects of disruptive communications attacks.

For example, a Russia-based attack could create a bot targeting real time Election Administration e-poll book voter registration verification for voters seeking to vote on Election Day.

The attack could be launched against every state and local jurisdiction using e-poll books configured to communicate in real time with local and state election databases.

This attack will work and be very hard to trace, isolate, and shutdown without throwing polling processes into complete chaos.

Can successful deceptive campaign **rumor-mongering** attacks be deployed using e-mails and instant messaging?

Yes. *E-mail and instant messaging can be used to start and spread rumors online.*

When e-mail rumors become widely distributed, resulting in the communication going viral, millions of users can be exposed to false information.

When this happens, correcting a deceptive message may require going beyond the confines of the Internet to speak to voters.

For example, if a message intending to create doubts in the

[101] Scott Berinato, "Attack of the Bots," *Wired News*, *available at* http://www.wired.com/wired/archive/14.11/botnet.html.

minds of voters regarding their right to participate in the election goes viral, then it might be very difficult to correct the information solely through Internet-based communications.

Can successful deceptive campaign **social engineering** attacks deploy e-mails and instant messaging?

Yes. *Voters make decisions about their participation in elections based on many factors.*

Deceptive campaigns can use social engineering to develop e-mail and instant messaging that appeal to certain voters based on social engineering questions.

For example, a message that students who have on-campus addresses like a P.O Box are prohibited from voting in the election held in their home state could suppress absentee voting among college-age voters.

Monitoring the click rate of those who view the message could inform social engineers on the best strategies to pursue in an e-mail or instant message attack.

E-mail and Instant Messaging Recommendations

SPAM, pharming, and phishing attacks are making e-mail more difficult to secure. To address some of these issues, e-mail users should avoid e-mails that come from new sources. Users should also be mindful of sharing e-mail with picture files, video links, or embedded links.

Most computer malware software is designed to take advantage of vulnerabilities in the Web browser and e-mail applications found in Microsoft Windows desktop operating systems.[102] Because of the overwhelming number of Windows based operating system users, malicious software applications disproportionately affect personal computers.[103] Macintosh and Linux boxes are personal computer options with better track records of not falling victim to malware attacks. For a list of privacy tools visit http://epic.org/privacy/tools.html.

- Election Administrators and Election Protection should:

[102] National Institute of Standards and Technology, Special Publication 800-69, GUIDANCE FOR SECURING MICROSOFT WINDOWS XP HOME EDITION: A NIST SECURITY CONFIGURATION CHECKLIST, *available at* http://csrc.nist.gov/itsec/SP800-69.pdf.
[103] *Id.*

- Work with the Computer Emergency Response Team to create a plan to deal with an e-mail or instant messaging denial of service attacks.

- Not rely on remote electronic poll book registration processes. Polling locations accessing remote data to verify the voter registration of voters may present other problems for the smooth provision of Election Day services.

- Have a complete copy of the voter registration lists for the jurisdiction and means to properly direct voters in need of information regarding correct polling locations.

- Election Administrators, Election Protection officials, and bloggers should be sure to check for updates for server software and desktop operating systems. Further, enhanced computer security software for desktop computers and network servers should be considered.

- Individual users should:

  - Contact Election Assistance programs
    - 1-866-OUR-VOTE or visiting http://www.866ourvote.org/,
    - The National Association of Secretaries of State at http://canivote.org,
    - The National Association for Latino Elected Officials at http://www.yaeshora.info/, or
    - The Election Administration Commission at http://www.eac.gov/voter_resources/contact_your_state.aspx for election related information on voter registration status, polling location, voter identification requirements, your rights as a voter, and hours of polling operations.

  - Refer others seeking accurate information on election participation to 1-866-OUR-VOTE or http://www.866ourvote.org/state/.

  - Not forward e-mail messages about specific voter participation rules to others, except as an opportunity to direct people whom they know to verify information with 1-866-OUR-VOTE or http://www.866ourvote.org/state or http://canivote.org.

  - Check for software updates for personal computer operating systems.

  - Know that there are alternatives for e-mail applications that can avoid some threats posed by many types of e-mail virus, worms, or mal-ware.

  - Not open files with attachments if the source of the e-mail seems suspicious.

- Use mail filters to mark unwanted e-mail from unknown senders as junk mail or spam.

- Not forward e-mail from unknown sources to people you know personally.

Polling Place Practices

Poll workers should remember that they received excellent training from their Election Administrators. The best precaution for poll workers to take to avoid or resolve problems is reviewing the training material provided to them before arriving at the polls on Election Day. News reports regarding voter fraud should be seen in the context of a heated election season. They typically start within a week of an election and quickly fade following the close of the election.[104]

Voting machines may cause some problems on Election Day. There are well-documented routine problems associated with each type of voting system deployed. Efforts to replace aging voting machines with newer models introduced new types of voting machine problems. In 2010 primaries, polling places experienced difficulties.

- During the September 14, 2010 primary, New York's problems included: machines not arriving on-time at polling places, some polling places opening late, machines being completely inoperable, and requirements that voters use paper ballots. [105]

- On August 27, 2010, in Harris County, Texas, a fire destroyed the county's voting machines, requiring the County Clerk to re-order machines and provide voters with paper ballots on Election Day.[106]

- In October 2010, a candidate's name was misspelled on a voting machine. The city's Election Board plans to have the error fixed by Election Day on November 2, 2010. The candidate's name is correctly spelled on the paper ballots.[107]

---

[104] Justin Levitt, THE TRUTH ABOUT VOTER FRAUD, The Brennan Center for Justice, November 9, 2007, available at http://www.brennancenter.org/content/section/category/allegations_of_voter_fraud/

[105] James Barron and David W. Chen, "Problems with Machine Voting in NYC primary," *The New York Times*, September 14, 2010, *available at* http://cityroom.blogs.nytimes.com/2010/09/14/problems-reported-with-new-voting-machines/; *see also* New York State County Boards of Election, VOTING RELATED PROBLEMS SEPTEMBER 2010 PRIMARY ELECTIONS, October 7, 2010, http://www.osc.state.ny.us/press/releases/oct10/100710.htm.

[106] Charlie Ban, "Fire Destroys Harris County, Texas Voting Machines," National Association of Counties, September 6, 2010, *available at* http://www.naco.org/newsroom/countynews/Current%20Issue/9-6-10/Pages/FiredestroysHarrisCounty,Texasvotingmachines.aspx.

[107] "Whitey' on machine ballots will be fixed,' upi.com, October 15, 2010, http://www.upi.com/Top_News/US/2010/10/15/Whitey-on-machine-ballots-will-be-fixed/UPI-57841287157741/.

These examples show that even with planning, the unexpected can occur, from either human error or technological malfunctioning. It is important for voters to be patient, poll workers to be vigilant in following polling procedures, and election administrators to plan for and implement policies that a voter who presents themselves at their polling location will be able to cast a ballot at that time. An effective defense is that election administrators prepare for Election Day by providing for secondary means for voters to cast a ballot on November 2, 2010.

Some states are beginning to enact laws that will help address these problems and create greater transparency.[108] Mandatory end-to-end security and election audit procedures are becoming common in many jurisdictions grappling with being responsive to voters regarding the conduct of public elections.[109] For example, California has passed a law requiring voting system vendors to disclose flaws in their machines.[110] Solutions to voting machine problems can include:

- automatic routine audits of paper records;
- parallel testing of voting machines;
- banning of wireless components on all voting machines;
- transparent and random selection procedures for parallel testing and audits;
- decentralized programming and voting system administration; and
- implementation of effective procedures for addressing evidence of fraud or error.[111]
- fully staffed polling locations with representatives from competition political parties with long standing ties and trust among constituent leaders and voters.

The chief solution, one that has yet to be fully implemented is 100% staffing at polling locations around the nation. Poll worker staffs must employ people from all walks of life that represent the people who will be served by their polling location on Election Day. The US democratic experience requires the participation of citizens not only as voters, but also as poll

[108] EPIC, E-DECEPTIVE CAMPAIGN PRACTICES 2010, Appendix C, October 26, 2010.
[109] Electronic Privacy Information Center, Manual Audit Report Takoma Park Maryland, November 19, 2009, available at http://epic.org/privacy/voting/takoma_park_audit.pdf.
[110] Thadeus Greenson, "A higher standard sought: New law to require elections equipment vendors to report flaws, errors and malfunctions," *Times-Standard*, October 2, 2010, http://www.times-standard.com/localnews/ci_16235064.
[111] Brennan Center for Justice, POLICY BRIEF ON ELECTRONIC VOTING SYTEMS, October 2006, http://www.brennancenter.org/content/resource/policy_brief_on_electronic_voting_systems; Lawrence Norden, VOTING SYSTEM FAILURES: A DATABASE SOLUTION, Brennan Center for Justice, September 2010, http://www.brennancenter.org/content/resource/voting_system_failures_a_database_solution/.

workers. The system will not sustain itself without an active, committed, and well-educated workforce to carryout Election Day.[112]

Conclusion

Prevention of electronic deceptive practices will be as difficult, or more so, than attempts to prevent those launched by traditional methods using landline telephone calls, direct mail, or knock and drop campaign efforts. The challenges of stopping electronic deceptive campaign practices are difficult because the source of the attack can be from any location around the globe, the launch of an attack can be timed to begin within hours of an election, and tracing the source of the attack can be time consuming and not yield actionable results. The unique features of the Internet that enable efficient distributed communication are exactly those that make it difficult to regulate. Thus users of the Internet – election officials, Election Protection, campaigns, and voters – need to be vigilant about electronic deceptive campaign practices.

Computer-based attacks may use software that activates on a significant pre-programmed date and/or time of day. For example, a computer virus or worm program could be timed to activate on the morning of November 2, 2010 – Election Day. An attack on computers that have visited certain politically oriented websites or downloaded campaign video, audio or graphics files can involve cookies applied during user visits. Malicious computer software can be used to launch deceptive campaign attacks that cause serious problems on affected computers by disabling or manipulating key applications like Web page update software.[113] Further, Web browsers and e-mail services on individual laptops or desktop computers can be made unavailable or manipulated. Malicious software might affect the functioning of cells phone or personal communication devices that access Internet information.

Computer users interested in protecting themselves from electronic deceptive campaign practices should know that software viruses, worms, Trojan horses, and rootkits are designed to damage computers. These malicious software attacks can infect personal computers when digital information is shared. Malicious computer software may also be specifically designed to spread itself to other computers sharing the same computer network. These malicious software files can be acquired through e-mail or by visiting Web pages, viewing video, audio, or other graphics-based files.

Deceptive campaign attacks that use malicious software can overload applications on infected computers to the point that the application or the computer system is disabled. The malicious software could be designed to block access to Web browser applications used to view Web pages. Coupled with other computer applications shared by organization users, this problem can be replicated throughout an organization. Consider the devastating impact of a large

---

[112] The State of Elections, Solving the Epidemic of Disappearing Poll Workers – Part 1: Young People, available at http://electls.blogs.wm.edu/2010/04/14/solving-the-epidemic-of-disappearing-poll-workers-part-1-young-people/ April 14, 2010.

[113] EPIC, E-DECEPTIVE CAMPAIGN PRACTICES REPORT: TECHNOLOGY & DEMOCRACY 2.0, Appendix A, October 2010.

number of election administration staff or Election Protection operations not having access to any Web-based information.

One of the topics not covered in the body of the report involves the relationships among federal and state e-government services that may present opportunities for deceptive campaigns. For example, the United States Postal Service offers online change of address service for a dollar per request.[114] Some state election administrators use the Postal Service's change of address database to verify the addresses of registered voters. There are also states now providing voter online changes of address services.[115] State and local election administrators should consider the special needs of victims of domestic violence in policy decisions on this topic, as making that information accessible could put those victims at risk. To combat deceptive campaign attacks based on change of address requests, Election Administrators should mail confirmation of change of address to the old address on the voter registration record along with information on how to **correct** incorrect information.[116]

In addition to the threats outlined in this report, there are also network failures, power failures, and other events that have nothing to do with attacks, but can disrupt Internet communications. Whether by design or accident, the best defense is to be prepared with accurate information on election participation and the means to deliver it to those who need it.

---

[114] United States Postal Service, Change of Address, *available at* https://moversguide.usps.com/icoa/flow.do?_flowExecutionKey=_c0D59EC03-DAAA-86C9-AD7B-1638C830222E_k0CAF4527-8D3A-D08F-DD1B-7D1620BB051D.

[115] Texas Secretary of State, Voter Registration Change of Address, *available at* https://www.texasonline.state.tx.us/NASApp/sos/SOSACManager.

[116] Association for Computing Machinery's Public Policy Committee, STUDY OF ACCURACY, PRIVACY, USABILITY, SECURITY, AND RELIABILITY ISSUES, available at http://usacm.acm.org/usacm/VRD/.

Appendix A

Malicious Computer Software

Malicious computer software comes in many forms:

"Viruses" are computer programs that might be designed among other things to cause an unexpected, or more likely an undesirable, computing situation.

"Worms" are computer programs that aggressively self-replicate and self-propagate and may spread to other computers sharing a network.

"Trojan horses" are malicious software that appears harmless, but in fact have bad effects on the proper operation of personal computers.

"Rootkits" are collections of computer files that are installed onto computers, possibly hidden within a video, picture, music, or graphics file shared among computer users or accessed online.

Action Steps – *Be Proactive in Protecting Your Personal Computer*

Early detection and response that is focused on mitigation are the best approaches to addressing the use of electronic deceptive campaign attacks designed to suppress voter participation. Computer users must be diligent in working to break the way that viruses, worms, and malicious software typically work. However, having taken action is no guarantee that nothing will happen. Acting will only reduce the risk that a computer might face from the type of deceptive campaign tactics discussed in this report.

Should deceptive campaign tactics be deployed for the November 2, 2010 election, the best approach will be to take the following steps to diminish the impact on voter participation:

- Voters who have early voting and no-excuse absentee voting should take advantage of these Election Day services. Voters who have voted may be less likely to be victims of deceptive campaign practices.
- Make sure software updates on personal computing devices are current. Windows desktop Web browser and e-mail applications are especially vulnerable to malicious software attacks because they are found on 90% of personal computers in use online. If you are using Windows' Internet Explorer or Outlook consider using alternative Web browsers (Firefox or Opera) and e-mail applications (Thunderbird or Eudora) or see: http://epic.org/privacy/tools.html.
- Take time **now** to learn about polling location and times for casting ballots in the November 2, 2010 election. A good resource on election related information can be found at http://www.866ourvote.org/ or call 1-866-OUR-VOTE or http://canivote.org.

- Voters who can take November 2, 2010 off should consider volunteering as poll workers through http://eac.gov, or Election Protection Efforts 1-866-OUR-VOTE by visiting http://www.866ourvote.org/.

- Election officials, campaigns, and Election Protection efforts should develop electronic deception detection strategies that include bloggers, individuals on social networking sites, federal agencies (e.g. FBI, CIA, NSA, DOJ), and other watch dog organizations.

- Rumors and misinformation are the fuel of deceptive campaigns. Blogs, YouTube, e-mails, VoIP, and instant messages can all each be used to spread rumors. Election administrators can take steps to combat rumors, see: http://www.elections.state.md.us/press_room/rumor_control.html.

    - On October 8, 2008, the Associated Press reported that Internet thieves created a replica of the YouTube site that was so well done that it could deceive experienced online users.[117]

- Election administrators and Election Protection efforts should develop an early warning system that is up and operational prior to the election. Principles to guide the formation of the system include:

    - Early warning systems must facilitate reliable communications among participants.

    - The list of participants should include election administrators, voter participation efforts, campaigns, and political parties.

    - Create a central clearinghouse for activity that may indicate a deceptive campaign attack.

    - Schedule regular discussions to evaluate the severity of any active attacks, and identify those needing responses.

- Define communication channels to alert people about attacks as well as fact check claimed attacks (to prevent spoofing) especially if the source of the information is a social networking site, e-mail, instant message, or phone call.

- Develop response protocols based on the source, content, and result of a potential deceptive campaign tactics.

    - Content providers should host alternative means of gaining access to critical information by making greater use of Web resources provided by Google, AOL, Facebook, Microsoft, Twitter, etc.

    - Create and test an email/SMS/social network message tree as a rapid response tool.

---

[117] Associated Press, "Hackers Malicious Fake YouTube Pages," D-2, October 13, 2008, *available at* http://www.sfgate.com/cgi-bin/article.cgi?f=/c/a/2008/10/12/BUHC13DNTI.DTL.

- Identify individuals and organizations to bridge the online/offline gap and bring the word out into the community.

Voters should be informed about details regarding their right to participate in election, voter purge rules, and polling location information. Election Administrators should consider the need to inform voters of the methods which will be used in sharing information related to changes in polling location and time for casting ballots.

Election Protection efforts include a national network of telephone incident intake centers that receive calls from voters who are in need of assistance with participation in public elections. The resources made available to voters include legal advice and court intervention when necessary. Incidents are logged into computer systems that can track and monitor election related incidents and may assist with early warning functions needed to prevent electronic deceptive campaign attacks. Coordination efforts to address the topics of this report should coordinate with these efforts.

The ability to plan is the best defense against potential electronic deceptive campaign attacks. The Internet is not owned or operated by any single entity, but is an ongoing global collaborative effort. There is more good than bad, but where people gather there are those with ill will who may act against the community's interest.

It is hoped that this report will aid voters, Election Administrators, and Election Protection efforts to have a successful Election Day.