E-Deceptive Campaign Practices Report:

Internet Technology & Democracy 2.0

Electronic Privacy Information Center

epic.org
ELECTRONIC PRIVACY INFORMATION CENTER
THE CENTURY FOUNDATION

E-Deceptive Campaign Practices Report: Internet Technology & Democracy 2.0

October 20, 2008

Executive Summary

Deceptive campaigns are attempts to misdirect targeted voters regarding the voting process for public elections. Election activity that would be considered deceptive could for example include false statements about polling times, date of the election, voter identification rules, or the eligibility requirements for voters who wish to cast a ballot. Historically, disinformation and misinformation efforts intended to suppress voter participation have been systemic attempts to reduce voter participation among low-income, minority, young, disabled, and elderly voters. Deceptive techniques deployed in the 2004 and 2006 general elections relied upon telephone calls, ballot challenges, direct mail, and canvass literature drops.[1] Some voters were told they would face arrest if they attempted to vote and had outstanding parking tickets or were behind in child support payments.[2]

Today, voters are relying more and more on Internet enabled communications to engage in political decision-making. Deceptive practices tactics that target e-mail, instant message, and cell phone users can compress the timeline for launching successful disinformation and misinformation attacks from days to hours or minutes. A key component of the 2008 Presidential Election is the use of Internet based communications to engage voters with a history of marginal participation rates in past elections.[3] EPIC identified electronic deceptive campaign tactics as a high priority in 2008.[4] The incident of electronic deceptive campaign practices in 2008 include:

> A series of bogus e-mails sent to Florida residents on the state's Voter Registration Verification Law, which erroneously informed voters that a no match against state databases would result in disqualification in voting;[5]
>
> Automated calls to North Carolina female voters misinforming them regarding their voter registration status;[6] and

---

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

[2] Ian Urbina, Democrats Fear Disillusionment in Black Voters, New York Times, available at http://www.nytimes.com/2006/10/27/us/politics/27race.html?pagewanted=all, October 27, 2006 John Trasviña, Testimony, Prevention of Deceptive Practices and Voter Intimidation, Senate Judiciary Hearing, available at http://judiciary.senate.gov/hearings/testimony.cfm?id=2798&wit_id=6514, June 7, 2007

[3] Pew Research Center for The People & The Press, Social Networking and Online Videos Take Off: Internet's Broader Role in Campaign 2008, available at http://www.pewinternet.org/pdfs/Pew_MediaSources_jan08.pdf, January 11, 2008

[4] Computers Freedom and Privacy, Tutorial, E-Deceptive Campaign Practices 2.0, available at http://www.cfp2008.org/wiki/index.php?title=E-Deceptive_Campaign_Practices:_Elections_2.0&redirect=no, May 20, 2008

[5] Joy-Ann Reid, Bogus E-mails Raise Anxiety Over Voter ID Law, available at http://www.sfltimes.com/index2.php?option=com_content&task=view&id=1993&pop=1&page=0&Itemid=42

[6] Page Gardner, Confusion Surrounding Robo Calls in North Carolina, April 30, 2008, available at http://www.huffingtonpost.com/page-gardner/confusion-surrounding-rob_b_99427.html

> Rumors and e-mails to Prince George's County, Maryland voters that claim that voter registration rules bar participation of those with home foreclosures.[7]

The Electronic Privacy Information Center's Voting Project with the funding support of the Century Foundation is publishing this report. The report reviews the potential for abuse of Internet technology in an 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 takes up consideration of malicious software in the form of viruses, worms, Trojan horses, or rootkits.[8] The report looks at the effectiveness of spoofing, phishing or pharming, denial of service, rumor-mongering, or social engineering deceptive campaign threats.[9]

The state and federal legal and policy companion report to this report is a collaborative effort by Common Cause and the Lawyers Committee for Civil Rights Under Law.

For comments or questions regarding this technology report:

E-Deceptive Campaign Practices Report:
Internet Technology & Democracy 2.0

Lillie Coney
Associate Director
Electronic Privacy Information Center
202-483-1140 x 111
http://epic.org/
http://votingintegrity.org

For information on the law and policy report:

E-Deceptive Campaign Practices Report:

Tova Wang
Vice President, Research
Common Cause
http://commoncause.org

---

[7] Associate Press, Foreclosure is no Bar to Voting Gansler says, available at http://www.baltimoresun.com/news/local/bal-md.briefs261sep26,0,1678664.story

[8] EPIC, E-Deceptive Campaign Practices Report: Internet Technology & Democracy, Appendix A, October 20, 2008

[9] EPIC, E-Deceptive Campaign Practices Report: Internet Technology & Democracy, Appendix B, October 20, 2008

Report Contributors

Lillie Coney is Associate Director with the Electronic Privacy Information Center (EPIC) in Washington, DC. She is the Public Policy Coordinator for the National Committee for Voting Integrity (NCVI). 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.

Juan E. Gilbert is the TSYS Distinguished Associate Professor in the Computer Science and Software Engineering Department at Auburn University where he directs the Human Centered Computing Lab. Dr. Gilbert's research team developed Prime III, an innovative, accessible voting system. He also has research projects in advanced learning technologies, spoken language systems and data mining. He earned his B.S. degree in Systems Analysis from Miami University, his M.S. and Ph.D. in computer science from the University of Cincinnati.

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. He is also the Chair of the National Committee for Voting Integrity, see: http://votingintegrity.org/.

Erik Nilsson chairs the Computing Professionals for Social Responsibility working group on computers and elections. He has researched and written on voting, elections, and technology since the late 1980's, and in 1994 worked for the Independent Election Commission of South Africa in the historic elections of that year. Erik is president of Insilicos, a biotechnology company.

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.

Bruce Schneier is an internationally renowned security technologist and the author of eight books -- including Beyond Fear and Secrets and Lies -- and hundreds of articles and academic papers. Over 250,000 people read his influential newsletter "Crypto-Gram," and his blog "Schneier on Security." Schneier is the Chief Security Technology Officer of BT.

Introduction

Twenty-First Century voters are experiencing a revolution in the way they engage with, and are engaged by, the electoral process. Election officials are using the Internet as a tool to enhance the information services provided to voters. Election protection efforts are 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 are using the Internet as a more efficient means of targeting voters for messaging and solicitation of financial support. And for the first time, individual voters are empowered by the Internet to speak directly to the electorate, candidates, and policymakers through their own messaging, which bypasses traditional media outlets such as television, radio, and newspapers. The Internet is unlike any other tool in human history because it is ubiquitous and available at little or no cost. The value added in cyberspace is that this multimedia communication forum is two-way and nearly real-time between the audience and the messenger. Actions by individuals, governments, partisans, and multi-national organizations can have a profound effect on the rights of citizens to participate in public elections.

In the early 1990s the Internet evolved from a text only communication medium to the web or World Wide Web we see today. In 2004, the Internet was first used in a substantial way to engage new voters, raise funds, and organize individuals for civic engagement. The 2004 Michigan campaign coordinator for the Kerry for President effort said, 'We'll have voter lists where we'll know more about individuals than we've ever known. We'll know their income level, what magazines they subscribe to, whether they're married.., what education they have."[10]
Web pages, blogs, e-mail, instant messaging, and YouTube are just a few of the ways the American electoral experience has changed in just four years.

Internet Communications and Deceptive Campaigns

Many companies, including Internet Service Providers (ISPs), search engine firms, and web-based businesses, monitor users as they travel across the Internet, collecting information on what sites they visit, the time and length of these visits, search terms they enter, purchases they make, or even "click-through" responses to banner ads. In the off-line world this would be comparable to, for example, having someone follow you through a shopping mall, 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, these diffuse pieces of information create highly detailed profiles of individuals. These profiles have become a major currency in electronic commerce where advertisers and marketers predict a user's preferences, interests, needs and possible future purchases using them. Many of these profiles are currently stored in connection with an assigned number or the user's Internet Protocol (IP) address, exposing users to risk of the information being linked to other information, such as names and addresses, making them

[10] Grand Rapid Press (Michigan), Here, here: a West Michigan Guest Speaker, page A19, June 24, 2004

personally identifiable. In 2006, the search records of 658,000 Americans were made public by America Online (AOL) demonstrating that the storage of a number as opposed a name does not necessarily mean that search data cannot be linked back to an individual. Although the search logs released by AOL had been "anonymized," therefore only identifying users by assigned numbers, news reporters easily matched user numbers with identifiable individuals.[11]

One of the key aspects of deceptive campaigns is voter profiling. Profiles are used to develop expectations on the behavior of individuals based on their activities, preferences for a wide range of products and services, personal associations, religious beliefs, political participation, type of work, neighborhood, place of birth, level of education, etc. The Internet offers a rich source of information on all of the means of traditional profiling with one added advantage: the collection of data can be constant and completely hidden from online users.

Voter Profiling

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 found on voter registration applications, voter history of participation, state issued professional licenses, and low-level elected office holders to create profiles. In 2006, it was reported that Voter Vault a Republican system contained data on 160 million Americans.[12] Democrats and Republicans campaign experts cite microtargeting as the technique used to take voter registration information and mine consumer data to build the perfect voter profile.[13]

Aristotle, an election data services company, manages one of the most sophisticated resources for voter profiling.

> "We [Aristotle] incorporate all of the information maintained by the election boards --- such as party affiliation, race, exact age, vote history and political districts into our files. You can target more effectively, and you can communicate more effectively."

In 2004, the first glimpse of the 21st Century political campaign emerged with the use of the Internet's WWW applications that supported fundraising, engaging, and mobilizing voters around social networking activities that advanced a candidate's efforts to seek public office.

In 2008, the move toward more sophisticated voter profiles is going far beyond the typical set of data found in traditional voter profiles, which included age, gender, race, income, education, political participation, and partisan affiliation. Few voters are aware of how much information about the details of their lives is in the hands of third parties. Law enforcement, businesses, and

[11] EPIC and Privacy International, Privacy and Human Rights, 2006

[12] Thomas Fitzgerald, Parties pin hopes on voter profiling, Bradenton Herald (Florida), page 3, November 2, 2006.

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

political campaigns are making great progress in mastering the ability to create profiles on individuals.[14] Each of the major political parties and their candidates are spending billions of dollars in an arms race to gain greater knowledge of the voters they seek to persuade. Aristotle, a company specializing in election services for candidates, characterizes what it does as mapping "the DNA of the electorate."[15]

> "In addition to the wealth of demographics Aristotle already provides for high level micro-targeting, you can now identify your voters based on their interests and hobbies. Aristotle maintains a list of over 5.4 million voters who hold hunting and fishing licenses, as well as individuals who subscribe to a wide array of magazine subscriptions including family, religious, financial, health, culinary and Do-It Yourself publications."

The company claims that for 25 years every elected occupant of the White House has relied on their services.

> "Aristotle offers high-quality voter matching services for political organizations, non-profits, PACs, campaigns, consultants, and governmental agencies. Aristotle will take your in-house file and append extensive information from our voter file, such as which individuals are registered to vote, age, party affiliation, voter history - including absentee voters - and individuals who are considered to be Super-voters. With Aristotle's Suppression Matching service, you can match your list to our voter file and pull out records that you may want to exclude from your database. This is beneficial for organizations who want to exclude known Democrats or Republicans from their list."

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 included:[16]

- In October 2006, 14,000 Latinos residents of Orange County California received a letter stating that it was illegal for immigrants to vote;

- In 2004:

    - A flyer attributed to the fictitious "Milwaukee Black Voters League" and distributed in African-American communities fraudulently stated that voters

[14] Michael D. Shear, Va. Gubernatorial Hopefuls Use Data to Zero In On Voters, page CO1, Washington Post, August 28, 2005, available at http://www.washingtonpost.com/wp-dyn/content/article/2005/08/27/AR2005082700990_pf.html

[15] Homepage, Aristotle, available at http://www.aristotle.com/

[16] Demos, Voter Suppression Tactics Could Mar 2006 Election, New Publication Finds, available at http://www.demos.org/page482.cfm

could not cast ballots if they had voted that year or if a relative had been found guilty of a crime;

- A memo written on bogus Lake County Ohio Board of Election letterhead erroneously claimed that NAACP voter registrations were not valid; and

- A Franklin County Ohio fake advisory informed voters that Democrats were to vote the day after the scheduled general election, while Republicans were given the correct date of the election to cast ballots.

The use of deceptive campaign tactics online significantly increases the number of potential victims. Further, the ability to identify a deceptive campaign may be more difficult because it may be launched within hours of the beginning of an election. 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 that deceptive campaigns will as well.[17]

The Challenge of Internet Enabled Political Participation

Internet political communications may make the application of existing state and federal law intended to regulate political activity more challenging to enforce.[18] This is true when the source of political communications is completely transparent to online users such as in the case with local and state election administration web sites, or official campaign web resources. However, 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. This is particularly true due to the structure and history of the Internet.

The purpose of the early Internet was to allow for the quick dissemination of results among researchers. Hence, it was designed to be robust and efficient; however, because a small community of individuals with a well-defined role used it, security was not a major concern. Later, as it became accessible to users for other purposes, and grew considerably in the nature of its scope and its users, 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. The fact that the Internet is spread across the world provides another challenge to legal regulation. Further, the 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.

---

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

[18] A Brief History of NSF and the Internet, available at http://www.nsf.gov/news/news_summ.jsp?cntn_id=103050

The enforcement of regulation that achieved the goals of secure and private physical communication in physical societies would likely be very intrusive in cyber-space unless designed carefully and supported by the active participation of users, nonprofits, governments, and commercial interests. As a result, the Internet will probably continue to grow in a largely unsupervised fashion in the near future; hence users may not be able to rely solely on the strict enforcement of state and federal laws to combat Internet deceptive campaign practices. This is not to say that users should not rely on public enforcement at all; but that individual users will need to take greater responsibility for security against these threats until business practices and government oversight functions evolve to meet the challenges of Internet communications. The good news is that there are practices that election officials, Election Protection efforts, and voters can employ to greatly reduce the chances that they will become victims of Internet deceptive campaign practices.

The strategies for accomplishing deceptive campaign practices are based on techniques that are well known in the Internet communication environment. The following are terms that are familiar to computer security and law enforcement experts that will be used to explain the potential for e-deceptive campaign threats to the 2008 general election. In the context of deceptive election practices "spoofing," "phishing," "pharming," "denial of service," and "social engineering" are tactics that can be used to deceive voters. In addition, "rumor mongering" can also impact voter participation.

- "Spoofing" involves a website claiming for example to be a State Election's office, but in fact has nothing to do with any official state government office. The content of the Web page may 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.[19]

- "Pharming" is a version of phishing, which involves the fraudulent use of legitimate domain names. Pharming attacks successfully hijack Get Out the Vote (GOTV), election administration, and Election Protection Web addresses and redirects visitors to imposter Web sites. This approach can also be used to change the voter's computer configuration so that typing a legitimate address will take the user to a fake Web site.

- "Denial of service" attacks can make voter information sites, GOTV efforts, or voter help hotlines unavailable 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.

[19] Congressional Research Services, Report to Congress, Internet Privacy an Overview of Pending Legislation, http://digital.library.unt.edu/govdocs/crs/data/2005/upl-meta-crs-7879/RL31408_2005Oct19.pdf, pages 18-19, October 19, 2005

- "Rumor-mongering" can involve planting stories that sweeps through blogs and into the mainstream media that the election has been cancelled or delayed by a week due to an emergency.

- "Social engineering" includes targeting poll workers with deceptive messages that cause delays in poll location openings or disrupt other election related services.

- "Google bomb" (or "link bomb") is an attempt to influence the ranking of a Web page through the creation of many links to the page solely for the purpose of elevating the page rank.

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.

Reaching Voters in 2008

Internet communications are not confined to computers. Web communications now include mobile phones, smart phones (iphones), personal digital assistants (Blackberrys), interactive television systems (TIVO), voice response systems, kiosks, and new applications for consumer appliances.[20] Political messaging can include VoIP, e-mail, instant messaging, Web pages, and blogs.

The Internet is global and it is not policed or owned by any single entity. There are basic rules for obtaining Internet or IP addresses, which are essential components of online communications. Today, the strength of the Internet as an invaluable tool for civic participation is without doubt the most significant development of election season 2008. The Pew Research Center report Social Networking and Online Videos Take Off states that 24% of Americans said they routinely use the Internet to keep informed about the election.[21]

Search Engine Requests

Search engines are a critical utility for Internet users. But there is a risk that, as an important election approaches, search engine results could be corrupted so as to provide misleading information to Internet users in an attempt to change the outcome of an election.

Most personal computer users employ Web browser applications (Internet Explorer, Safari, Opera or Firefox) to assist with accessing Internet search engine service providers (Google.com, AOL.com, Yahoo.com, Ixquick.com). Search terms entered into search engines

[20] About W3G, Goals, available at http://www.w3.org/Consortium/mission

[21] Pew Research Center for The People & The Press, Social Networking and Online Videos Take Off: Internet's Broader Role in Campaign 2008, available at http://www.pewinternet.org/pdfs/Pew_MediaSources_jan08.pdf, January 11, 2008

can reveal a great deal about the user such as medical issues, associations, religious beliefs, political preferences, sexual orientation, and financial demographic information. In 2005, more than 60 million American adults used search engines on a typical day.

For example, search engines capture a great deal of information from online users. Some of the more resourced Internet search engine service providers provide other opportunities to collect data on individual users:

- Google Desktop: 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 undefined period of time, with some service providers establishing 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 users can create content on locations or addresses;
- MySpace, Facebook, Twitter, LinkedIn, and Google Orkut provide social networking tools that store personal information such as name, location, relationship status, etc.; and
- Google Video/YouTube collects information by IP address on the videos watched by users.

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

Search Engine Requests Deceptive Strategies

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

Can deceptive campaign **phishing or pharming** attacks be deployed through user search engine requests? **No**.
This approach would be inefficient in suppressing voter participation among a large number of targeted voters.

Can effective deceptive campaign **denial of service** attacks be deployed in conjunction with search engine requests? **Yes**.
This type of attack is possible. Effective denial of service attacks mean that demands to view a page exceed the ability of the Web page host to provide access to requesters. Because of the widespread use of broadband computing service, allowing 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. Basically the 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 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.

Can effective deceptive campaign **rumor-mongering** attacks be deployed using search engine requests? **Yes**.
Search engine function is in part based on the meta tag, header information that is part of each Web page. Web content creators use meta tag information among other things describe the type of information found on a page. Web search engine service providers use meta tag information to help them determine how their search engines will rank the page. For example, search engine requests for "polling locations Pennsylvania" may fool a user into believing that only the most relevant and accurate pages will be provided first.

Can effective deceptive campaign **social engineering** attacks use Web search engine requests to misdirect voters? **Yes**.
Searches can provide information on candidate preference, issues of interest, residential neighborhood, social, or cultural interests, which could be used by social engineers to develop Web content that increase the likelihood that certain voters will select links taking them to deceptive campaign information. "Google bomb" is a method of manipulating search engines to raise the rankings of Web pages with humorous or political content.[22]

Search Engine Requests Recommendations

- Internet Search Engine Providers 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, MSN.com, 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 Web sites to be sure they are at the top of the rankings for the topics sought.

[22] Wikipedia, Google Bomb, available at http://en.wikipedia.org/wiki/Google_bomb

- Communicate with voters through the media to direct them to Web pages for information on the November 4, 2008 election.

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

- Individual users should:[23]

  - Verify the correct spelling for search requests or individual URLs (Web address),

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

  - Some search engines allow the use of Boolean searches i.e. AND, OR, NOT, etc to narrow the search,

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

  - For election related information on voter registration status, polling location, voter identification requirements, and hours of polling operation contact Election Protection by either calling 1-866-OUR-VOTE or visit http://www.866ourvote.org/

Search Engine Results

Internet search engines, such as those offered by Google, Yahoo, AOL, Ixquick, and Microsoft's MSN are the primary means employed by users to find online content. The order of the pages that are served to Internet users based on search request can involve more than the search term entered. Internet search engine service providers also employ proprietary analysis and consideration of advertising dollars to help determine the order of pages. Web advertisements often appear as the first selections on the search results page. Online advertising is not regulated and is often the first results provided to users.

New technology may bring deceptive practices on-line by exploiting the way individuals look for election related information. Search histories can reveal preferences and political interests. Search engines often retain user's search histories. Also, the histories are retained on the user's computer and may be accessible to spy ware found on websites or hidden in e-mail attachments, video, or audio files. Further, mal-ware or malicious software can alter the stored Web address history data by replacing it with incorrect information.[24]

---

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

[24] EPIC, E-Deceptive Campaign Practices Report: Internet Technology & Democracy, Appendix A, October 20, 2008

Search engines may store user search terms in connection with their Internet Protocol (IP) address, a unique string of numbers that identifies each individual computer connected to the Internet. When users submit search engine Web requests, service providers may automatically log the user's Web request, IP address, browser type, browser language, the date and time of the request and one or more "cookies" may be installed on the requester's computer that may serve to uniquely identify the user. A cookie is a small piece of code that can be stored on a user's computer by a host Web site. Tracking may also involve monitoring the activity of visitors once they leave Web pages that deploy cookies. The cookies used by political Web sites, blogs, or Web videos, etc can be used to target Web attacks that affect computers hosting the cookies associated with specific Web activity. Cookies also include dates that they should be retained, which can be a few days, weeks, months, or years.

Users' Web requests are often retained by the Internet search engine service providers, and in many cases does link personally identifiable IP addresses with their search requests.

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. 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 Web site 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 i.e. bookmarked e-addresses or the cache memory of Changing the users "host file," which is a directory of Internet addresses, which can be edited to direct user Internet address requests to fake sites. False Web addresses might appear in every way to be the Web site the user expects to see, but might in fact provide false information. 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 unflattering impersonations of legitimate 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 providing search results to deceptive Web sites. 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. 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 in part based 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 to users. Meta tag data provides information to search engines on 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 search engine data could be used to avoid the intended purpose of search engine request that the user is seeking. For example, meta tag information might use "polling location," "election day assistance," "voter registration," "Virginia," "Pennsylvania," "Florida," etc. While the content of the pages could in fact provide rumor-mongering fodder such as "terrorism plot on Election Day," "Election cancelled due to candidate illness," 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 neighborhood can provide information to social engineers to develop Web link information that increase 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 possible posting of new Web content pages that attempt to deploy deceptive campaign information about the November 4, 2008 election.

- Election Administrators and Election Protection should:

    - Know how to contact the top ranked Internet Search Engine Providers Google.com, MSN.com, 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:

    - For election related information on voter registration status, polling location, voter identification requirements, your rights as a voter, and hours of polling operations: contact Election Protection by either calling 1-866-OUR-VOTE or visit http://www.866ourvote.org/.

    - 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 this year is November 4, 2008.

    - Ensure that personal computer internal clock date and time settings are current when Daylight Saving Time begins on Sunday, November 2, 2008.

    - Check for software updates for their personal computer's operating system i.e. Windows, Macintosh, Linux, etc.

    - 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.

- Some search engines allow the use of Boolean searches i.e. AND, OR, NOT, etc to narrow the search,[25]

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

Social Network Sites

Social network sites, such as MySpace, Facebook, and BlackPlanet have become established forums for keeping in contact with old acquaintances and meeting new ones. Users can create their own Web page and post details about themselves: 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, and they also play a significant role in younger activists' political participation.[26]

One important characteristic of social network sites in 2008 is the presence of very large "groups with hundreds of thousands or even millions of users. Most people simply join to show their affiliation; many, however, are much more active. The 750,000 people participate in "One Million Strong for Barack Obama" Facebook group, for example, have been active in "get out the vote" and know your rights work, phone banking, fundraising and other activities.[27]

One straightforward 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 4, 2008 election. The first step would be to identity potential confederates, which is made easier because sites like Facebook and MySpace allows the general public to search its database of members, using search terms such as a name, e-mail address, or school, in many cases filtering information by country, state, and even to a postal code. If users included in the search results allow searchers to view their full profiles, additional information such as occupation, hometown, sexual orientation, ethnicity, and religion is also likely to be available.

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

---

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

[26] See for example the March 2008 book *Millennial Makeover: MySpace, YouTube, and the Future of American Politics*, Winograd and Hais; website at http://www.millennialmakeover.com/

[27] "Cognitive Diversity in the 2008 US election", March 2008, and A One Million Strong Facebook moneybomb!, October 2008, Jon Pincus, *Liminal States*; http://www.talesfromthe.net/jon/?p=111 and http://www.talesfromthe.net/jon/?p=231

Other approaches to using groups for deception are possible as well, for example setting up a group that starts by providing accurate information, and projects a particular political perspective that would appeal to targets for the deceptive campaign. The group can cultivate and encourage greater participation based on its content. The deceptive campaign could be launched a day before the election using a message that is false or misleading to group participants.

Social network sites are also idea for viral message spread, for example by putting deceptive information on a user's profile. This gives the potential of deceiving not only the user who's being directly targeted, but also all of his and her friends who will see the information on the profile. Facebook and MySpace "feeds" offer similar viral possibilities. An important point underlying these attacks is that online "friend" relationships may solely be based on limited remote communication. The level of trustworthiness placed in the information shared among friends can be used to spread misinformation. A mixed social network/e-mail campaign, combining this with more traditional e-mail deception, could reinforce false information from apparently-independent sources.

More positively, social network sites also have the ability to counter deceptive practices by getting the word out. The Obama campaign, for example, has released a "debunking the myths" video on YouTube, which makes it easy for supporters to get the word out online. The very rapid Internet information-sharing and discussion typical in these environments can surface and expose deceptions; and the same viral mechanisms can be used to spread the facts instead of the falsehoods. Building on Color of Change's Video the Vote work in the 2004 election, and partnering with existing more traditionally-based organizations, grassroots election protection campaigns such the Twitter Vote Report and Voter Suppression Wiki are attempting to use social networking to engage large numbers of activists in helping to fight deceptive campaign practices.

Social Networking Sites Deceptive Strategies

Can effective deceptive campaign **spoofing** attacks be deployed through Social network sites? **Yes**.
Social network sites promote participant hosting of interest groups and events to engage and inform users on a wide range of topics. For example, a group "Progressives or Change" or "Conservatives for McCain-Palin" could issue invitations based on registered user profiles. Social network sites also allow 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 party or entity. 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. These Internet resources also rely on e-mail to inform participants of new sites and changes on existing sites. Further, the e-logo of Election Protection, a State Election Administrator, or a Campaign could be used to create content. For more information on this topic, see the Law and Policy volume of the e-Deceptive Campaign. For example, a social networking page is created by a deceptive campaign effort that employs the logo for the Virginia State Board of Election that provides a link to a page on polling location searches.

Can effective deceptive campaign **denial of service** attacks be deployed against or by using social network sites? **Yes.**
Large social network sites typically have the capacity to serve millions of users, and so while the amount of computing resources to overwhelm these services is possible, it is unlikely because it would threaten the first goal of deceptive campaigns—stay below the radar of traditional media. 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 network sites would be fertile ground for encouraging deceptive campaign rumor-mongering. Fact checking services are not part of the social networking experience. Many organization and election officials may be unaware of this free resource for reaching voters in 2008. For example, a message designed to turn off voters to the election, or spread misinformation about the right to participate can spread false rumors using this Internet service. A global message can be delivered to participants in a group or event hosted on a social network site.

Can effective deceptive campaign **social engineering** attacks use social network sites? **Yes**.
Social network sites can promote the targeting of social engineering messages to engage voters who are supportive of a particular candidate or issues. This deceptive campaign strategy may be particularly effective 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.
- Administrators and members of large groups on social network sites should be on the lookout for deceptive information; collaborate with legitimate source of voter information (i.e. Election Administrators and Election Protection), and support their 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 setting from default privacy settings on individual accounts.
    - Set 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 any special equipment or high speed Internet service.

VoIP Political Robocalls

Routinely, political campaigns use telephone banks or call centers to communicate persuasion, fundraising, and other political messages to voters. VoIP can be deployed to deliver similar political telephone messaging from any location in the world at a fraction of the cost. The added challenge of VoIP in the area of e-deceptive campaign practices is that it 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 source of a call.

For example, Instant Call Blaster is a commercial robo VoIP based call service that advertises that it can contact thousands of telephone numbers "in a fraction of the time" and "for pennies a VoIP call."[28] Further, the company claims that the service can be established through an Internet application process that can be completed in minutes, and begin making calls within seconds. The company has a service that targets political campaign messages called "Political Blast."[29] The company claims that a list of phone numbers can be installed with a click of a mouse. Prospective clients are told that they can launch "a call campaign going in a matter of seconds."

The Federal Election Commission currently regulates campaign telephone banks by stipulating that they must contain disclaimers clearly stating if a committee paid for the communication.[30] However, the regulation explicitly states that it does not regulate Internet communications transmitted over telephone lines.

The potential for e-deceptive campaign messages and VoIP telephony can 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 status can be effective in misdirecting voters regarding 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.

---

[28] Instant Call Blaster, Antmore Technologies, available at http://www.instantcallblast.com/

[29] Political Blast, Install Call Blaster, Antmore Technologies, available at http://www.instantcallblast.com/servicepolitical.php

[30] Federal Election Commission, Title 11, Chapter 1, Section 100.28 Scope and Definitions, Telephone Bank, (2 U.S.C. 431(24)) http://edocket.access.gpo.gov/cfr_2008/janqtr/11cfr100.28.htm
Federal Election, Title 1, Section 100.17, Scope and Definitions, Clearly Identified (2U.S.C. 431(18)) http://edocket.access.gpo.gov/cfr_2008/janqtr/11cfr100.17.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. For example, a telephone calling effort can be sourced from any where in the world. The calls can be completely automated (i.e. a taped message) or caller operator supported. The message can 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. For example, 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? **No**.
Pharming and Phishing is restricted to e-mail and Web browsing activity.

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.[31] *The attack was effective in jamming the incoming call lines to local fire station providing voters with free rides to the polls. 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. For example, a VoIP attack's goal could be to occupy every available phone number so that legitimate calls cannot get through.*

[31] John DiStaso, Dems, GOP settle phone lawsuit, The Union Leader, page A1, December 2, 2006

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 nearly impossible ability to tie an entity to the calls made. VoIP can be used to start new or spread old rumors "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," or "New polling location hours due to flooding at the polls."

Can effective deceptive campaign **social engineering** attacks be deployed using VoIP Internet telephony? **Yes.**
Social engineering is as effective as the skills of the attacker to convince 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 would be a social engineering attack to obtain information from voters under a false pretext. This attack has been used in the past against registered voters.[32]

VoIP Recommendations

The potential for deceptive VoIP telephone banks is high. Further, this highly active election season means that 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.

- 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 personal during critical election periods.
  - Repeat often the dates for early voting and the very important date of the general election November 4, 2008.
  - Encourage voters to seek out information on voter identification requirements, poll locations, and polling hours **now**—1-866-OUR-VOTE or http://866ourvote.org.

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

- Internet users should:
    - Vote early if that option is available to them.
    - Learn their voter registration status, voter identification requirements, polling location, polling hours by contacting Election Protection at 1-866-OUR-VOTE or http://www.866ourvote.org/.
    - Know that the last day to cast a vote in the General Election is November 4, 2008.

Web Advertising and Behavioral Targeting

Online advertising has emerged as an influential tool for online revenue generation for Internet Service Providers (ISPs). The term "micro-targeting" has emerged as the catchall phrase to encompass all of the activity that is employed by ISPs and advertisers to spy on Internet users. However, most Internet consumers are unaware that their online activity may be monitored for the expressed purpose of serving up advertisements or building user profiles.[33]

On May 14, 2008, customers of Charter Communication, a broadband Internet service provider, reported receiving notices that the company would soon begin performing Deep Packet Inspection (DPI) of their Internet traffic.[34] DPI employs techniques to read the meta data header information for individual packets then uses the information obtained to change how an Internet service provider will manage the entire communication exchange.

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 is 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 searching for keywords like McCain or Obama, phrases or strings such as net addresses or e-mail accounts. It can then record or retransmit for further review anything that fits its search criteria.[35]

In addition, inspection of the header information for IP packets in transit between requester and providers of Internet information can inform the inspector of the source, type, and intended destination of an Internet communication. This can also be used to manipulate destination and routing of requests sent by Internet users.

---

[33] Digital Marketing, Privacy & the Public Interest, Center for Digital Democracy, available at http://www.democraticmedia.org/current_projects/privacy
[34] NebuAd, web page, available at http://www.nebuad.com/
[35] Electronic Privacy Information Center, Privacy and Human Rights International, pages 62-63, 2005

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 network discrimination of the short identified.

Web Advertising and Behavioral Targeting Deceptive Strategies

Can effective deceptive campaign **spoofing** be deployed using Web advertising or behavioral targeting? **Yes**.
Ad space is managed by Internet Service Providers. Ads are typically the first links provided to users seeking information, Election Protection, Election Administrators, Internet Service Providers should be aware that attempts to spread deceptive information by appropriating the name or Web identity of trusted entities is possible. Further, search engine providers do not, nor should they, regulate the content of Web pages that are provided by advertisers. Also, there is no effective regulation on the type of information that Web page owners might collect from visitors. Web content creators may also host advertisements, which track visitor activity.

Can effective deceptive campaign **phishing or pharming** e-mail attacks be used in conjunction with Web advertising and behavioral targeting? **No**.
Although pharming and phishing attacks might use Web advertising and behavioral targeting to develop a list of potential victims it would not be an efficient means for launching a deceptive campaign attack on voters.

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 a 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. For example, some voters would be turned off by a very negative campaign or personal attacks, which would be sensitive to messages that are highly negative. The deception would be to falsely attribute the source of the attack to an innocent candidate or party.

Can effective deceptive campaign **social engineering** attacks use 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, an advertiser could place pro-progressive or pro-conservative ads and collect information on users who view the ad. With this information deceptive campaigns could better target messages for intended recipients. For example, Web sites for persons sharing fundamentalist conservative beliefs may visit a popular Web site and select an ad on books, which then tracks the users online activity.

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.

Web blogs and Web pages can accomplish more than 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. John McCain's campaign established a web site, "John McCain's Truth Squad," to defend his military record.[36] Barack Obama's campaign established a Web page, "Fight the Smears, to correct disinformation and misinformation attacks."[37]

Web blogs and Web pages may also support cookies or flash cookies, which can facilitate the tracking of users while online.[38] 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 host advertising that use cookies to tag visitors to their sites they can also deploy malicious software that can do harm to personal computers.[39]

[36] John McCain for President, Truth Squad, available at http://www.johnmccain.com/truthsquad/
[37] Google, Search Engine, "Fight the Smears," available at http://www.google.com/search?q=obama+stop+the+smear+site&ie=utf-8&oe=utf-8&aq=t&rls=org.mozilla:en-US:official&client=firefox-a
[38] EPIC, Flash Cookies, available at http://epic.org/privacy/cookies/flash.html
[39] *id.* EPIC, E-Deceptive Campaign Practices Report, Appendix A

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 popular political blog's Web site might be spoofed through a political advertisement that is presented along with results from a search request. The same thing could 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**.
There are about a dozen top ranked domestic political blogs and opinion blogs online and more starting up each day.[40] *They are sources of political commentary and headline breaking news. Many online users rely on blogs for news information and reliable commentary in the fast paced twenty-four hour news oriented medium. A deceptive campaign rumor attack if conjoined to a popular blog can have significant negative implications for online users who intent to vote on November 4, 2008. Rumors have a powerful life online.*[41]

Can effective deceptive campaign **denial of service** attacks be deployed in conjunction with Web blogs or Web pages? **Yes.**
This type of attack would be highly unlikely, however there are several approaches that should be considered. 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.

[40] Privacy08.org, Political Privacy Blog, available at http://privacy08.org/
[41] Daniel J. Solove, Understanding Privacy, Cambridge 2008

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 spreads 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. Social engineering may appeal more to the heart than the minds of voters to engage them in acting 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. In 2008, campaigns are targeting 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. One out of every six Americans have gotten or sent e-mails with family and friends and 14% of them report they have gotten e-mails from political groups or organizations regarding the campaign.[42]

E-deceptive campaign e-mail attacks may take the traditional form of deceptive campaign tactics i.e. Democrats vote on November 4, 2008 and Republicans vote on another day. However, the sophistication of these high-tech consumers as voters will require that an effective attack be creative and well planned. An attack in this case may not intend the recipient to be the victim. For example, an attacker may send an e-mail that informs the recipient that they should call the local election administrator's office to verify registration status or confirm a polling location. The e-mails that appear to come 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.

[42] Pew Research Center for The People & The Press, Social Networking and Online Videos Take Off: Internet's Broader Role in Campaign 2008, page 8, available at http://www.pewinternet.org/pdfs/Pew_MediaSources_jan08.pdf, January 11, 2008

The more successful deceptive e-mail attack is one that can engage 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 doubt. First, voter identification requirements, straight party voting, or other rules governing voter participation are state specific, while Internet e-mail is not. For example, and e-mail stating that voter identification may be a problem on election day therefore bring a Social Security card, birth certificate, drivers license, or state ID sounds plausible, but it is in fact a deceptive message. 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. For example, targeted voters may be told how to cast a "straight party" ballot for all Republican or Democratic candidates. They may be told erroneously to vote both for Barack Obama and the straight Democrat party selection. The straight party ballot on e-slate voting system might be cancelled, thus voiding the ballot.[43] Election Protection provides a reliable source for information on voting —1-866-OUR-VOTE or http://www.866ourvote.org/state/.[44]

Another serious line of attack may target poll workers who are key to the proper conduct of public elections. Messages that may be intended to misdirect poll workers regarding their role in opening polling locations, rules regarding voter participation, or 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 may work to the disadvantage of e-mail users.

Two successful spoofing attacks routinely used by Internet thieves are phishing and pharming. Internet thieves use phishing and pharming techniques to acquire sensitive information such as logons and passwords; credit card numbers and PINs (Personal Index Numbers); and electronic bank account information by posing as legitimate businesses.

Phishing deceptive campaigns can involve "social engineering" tactics that employs the victim's cooperation in the success of the attack. [45] 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

---

[43] Kelly Shannon, Democrats cry fool over suspicious e-mail, Dallas Morning News, October 15, 2008, available at http://www.dallasnews.com/sharedcontent/APStories/stories/D93R2C780.html

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

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

user's computer cache or the stored registry of domain name system (DNS) addresses. When users visit a Web site posing as a legitimate election information resource malicious software might be installed onto the user's machine without any immediate visible effects.[46]

Malicious software can be designed to access personal e-mail address books or sent e-mail outboxes.[47] 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 users 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 repetitious 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 determine e-mail messages that are legitimate and those that are a result of malicious software. The disruption of the e-mail system will continue until computers are made immune to the malicious code, and it is removed from every infected computer.[48] 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 e-mail or Instant message that voters in Indiana must activate their voter registration in order to vote on Tuesday, November 4, 2008, might seem plausible, but would be a deceptive communication.

[46] EPIC, E-Deceptive Campaign Practices Report: Internet Technology & Democracy, Appendix A, October 20, 2008
[47] *id.*
[48] *id.*

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 often the source of the communication must be previously identified as being objectionable. The ease of creating e-mail addresses coupled with creative "subject" header descriptions may increase the likelihood that a deceptive e-mail will be opened by the recipient. 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 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. Eastern Europe, Pakistan, China, and Russia are locations where denial of service attacks have been launched. Botnets are the tool of choice for online denial of service attacks.[49] *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, be very hard to trace, isolate and shutdown without throwing polling processes into complete chaos.*

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

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 the ability to correct a deceptive message may have to go beyond the confines of the Internet to speak to voters. For example, if a message intending to create doubts in the 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. The use of e-mail or instant messages to better understand voter motivation can be one tool to assist deceptive campaign efforts. Deceptive campaign can also use social engineering to develop e-mail and instant messaging that appeal to certain voters based on social engineering ques. 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 navigate. 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. There are several e-mail programs that are provided at no charge to consumers.

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.[50] Because of the overwhelming number of Windows based operating system users, malicious

[50] 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

software applications disproportionately affect personal computers.[51] Macintosh, Linux boxes are personal computer options with histories of having a better track record for not falling victim to malware attacks. For a list of privacy tools visit http://epic.org/privacy/tools.html.

- Election Administrators, Election Protection should:
    - Work with the Computer Emergency Response Team to create a plan to deal with a e-mail or instant messaging denial of service attacks.
    - Election Administrators should 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 its jurisdiction and means to properly direct voters in need of information regarding correct polling locations.
- Election Administrators, Election Protection, and Bloggers should be sure to check for updates for server software and desktop operating systems. Further, computer security software for desktop computers and network servers should be considered.
- Individual users should:
    - Learn in advance of Election Day voter identification requirements for their state, polling location, and hours of operation by contacting Election Protection at 1-866-OUR-VOTE or http://www.866ourvote.org/state/.
    - 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, but use the messages on this topic as an opportunity to direct people whom they know to verify information with 1-866-OUR-VOTE or http://www.866ourvote.org/state.
    - 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.
    - As a rule do not open files with attachments if the source of the e-mail is specious.

[51] *id*

- Use mail filters to mark unwanted e-mail from unknown senders as junk mail.
- Do not forward e-mail from unknown sources to people you know.

Conclusion

Prevention of electronic deceptive practices will be as difficult, or more so, than attempts to prevent those launched by deceptive landline telephone calls, direct mail, or knock and drop campaign efforts. The challenge 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.

For example, there are computer based attacks that use software that may be activated by a date and/or time of day that is significant. For example, a computer virus or worm program could be timed to activate on the morning of November 4, 2008 – Election Day. An attack on computers that have visited certain politically oriented Web sites 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.[52] Further, Web browsers, and e-mail services on individual laptop, or desktop computers can be made unavailable or manipulated. There is also the real potential for malicious software that can effect the functioning of cell phone or personal communication 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 computer. These malicious software attacks can infect personal computers when digital information is shared. For example, the possibility of getting a virus mainly exists when accessing a computer input device such as compact disks (CDs); digital video device (DVDs); thumb drives or when downloading a calendar, saving address book files, or pictures from a personal digital device i.e. Blackberrys, or cell phones. These malicious software files can be acquired through e-mail or by visiting Web pages, viewing video, audio, or other graphics based files.

For example, an employee of an organization might use their work computer to access a Web site. The Web site, without the user's knowledge can store malicious software onto the machine. Malicious computer software is designed to infect an individual computer, and may be specifically designed to spread itself to other computers sharing the same computer network. Deceptive campaign attacks that use malicious software can overload applications on

[52] *id., EPIC, E-Deceptive Campaign Practices Report, Appendix A*

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 replicated throughout an organization. What would be the impact of a larger 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 are 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.[53] Some state election administrators use the Postal Services' change of address database to verify the addresses of registered voters. There are also states now providing voter online changes of address services.[54] State and local election administrators should consider the special needs of victims of domestic violence in policy decisions on this topic. 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.[55]

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.

[53] 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

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

[55] 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 flavors such as:

"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 code that appear 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 is the best approach to addressing the use of electronic deceptive campaign attacks designed to suppress voter participation. Working to break the way that viruses, worms, and malicious software typically work takes effort on the part of computer users. However, taking action is no guarantee that nothing will happen. Acting will only reduce the risk that a computer might face regarding the type of deceptive campaign tactics discussed in this report.

Should deceptive campaign tactics be deployed for the November 4, 2008 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.
- Ensure that internal clocks of computing devices are current the morning of Sunday, **November 2, 2008** when **Daylight Saving Time** begins. Although electronic voting

systems are not the subject of this report, it is worth noting that internal clocks for computing devices may be affected by the transition to Daylight Savings Time.

- Take time **now** to learn about polling location and times for casting ballots in the November 4, 2008 election. A good resource on election related information can be found at http://www.866ourvote.org/ or call 1-866-OUR-VOTE.

- Voters who can take November 4, 2008 off should consider volunteering as poll workers http://eac.gov, or with Election Protection Efforts 1-866-OUR-VOTE or visit 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 Associate Press reported: that Internet thieves create a replica of the YouTube site that was so well done that it could deceive experienced online users.[56]

- Election administrators and Election Protection efforts should develop an early warning system that is up and operational prior to the election; participants should include state and local election officials, Internet Service Providers, campaigns, Election Protection organizations, media organizations, political Web blog publishers, election technology advocacy organizations, election technology experts, human factors experts, and voting advocacy organizations:

    - 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.

---

[56] Jordan Robertson, Fake YouTube pages used to spread viruses, Associated Press, available at http://www.sfgate.com/cgi-bin/article.cgi?f=/c/a/2008/10/12/BUHC13DNTI.DTL, October 8, 2008

- Develop response protocols based on the source, content, and result of a potential deceptive campaign tactics.
    - Information 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 for rapid response tool.
    - 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 on 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 Electronic Privacy Information Center (EPIC) is pleased to have worked on this topic by first hosting a discussion at the 2008 Computers Freedom and Privacy meeting. 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 users, Election Administrators, and Election Protection efforts to have a successful Election Day.

Appendix B

E-Deceptive Campaign Practices Technology Check List

	Search Engine Requests	Search Engine Results	Social Networking	VoIP	Web Advertising/ Behavioral Targeting	Web Blogs/Pages	E-mail/IM
Spoofing Attacks	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Phishing and Pharming Attacks	No	Yes	Yes	No	No	Yes	Yes
Denial of Service Attacks	Yes	Yes	Yes	Yes	No	Yes	Yes
Rumor-Mongering Attacks	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Social Engineering Attacks	Yes	Yes	Yes	Yes	Yes	Yes	Yes

Indication that a particular technology could be used in a deceptive campaign attack does not equate with effectiveness or efficiency in economies of scale. In other words, the acknowledgement that a particular application of Internet technology could be used in an attack **does not** mean that it is the best approach for an effective strategy intent on suppressing voter participation among Internet users.