

Insight to Security

State of Idaho, Office of the CIO, Cyber Security Newsletter



Avoid Phishing Scams



Expect "Block the Vote" E-mail, Web & Phone Scams

(from Dark Reading)

The Electronic Privacy Information Center (EPIC) predicts that malicious people are likely to conduct Website spoofing, fake VOIP call blasts, phishing, and denial of service attacks - all to suppress blocks of voters.

Dark Reading writes that an EPIC reports shows that these vicious techniques are likely from now through the election in order to suppress voters or blocks of voters. Because of this unusually hotly-contested Presi-

dential election, these techniques could cause some real voting problems: spoofing voting and campaign Websites, fake voice-call blasts via VOIP, phishing, and denial-of-service attacks on legitimate polling Websites.



According to the report, there have been online attempts to disrupt election activity for specific blocks of voters. EPIC's [E-Deceptive Campaign Practices Report](#) (more on page 2)

In this Issue:

"Block the Vote" Scams 1,2

Employee Risky Behavior 3

Facebook Malicious-ware 4

BBB Phishing Scam 5

Awareness Opportunities 5

Expect “Block the Vote” E-mail, Web & Phone Scams (continued from Page 1)

describes these in detail. Phony emails were sent to Florida voters stating that they would be unable to vote if their ID didn't match a state database; “robo-calls” went to women voters in North Carolina with false information about their voter registration status; and fake emails were sent to voters in Maryland saying they would be barred from voting if their home was under foreclosure.

Voter suppression campaigns traditionally have used misleading telephone calls, direct mail, and mass literature drops designed to confuse or inhibit voters from casting their ballots. Typical tricks include spreading phony information or rumors about polling times, the election date, voter-identification rules, or voter eligibility. But with voters using the Internet more for researching and supporting their voting decisions and logistics, the threat of online deception campaigns against voters has become very real this year. Expect email, instant messaging, VOIP, and cell phones in an attempt to rapidly and widely spread misinformation to voters and to disrupt the election process, according to the EPIC report.

Malicious people can easily determine how best to target individual voters using information on the Internet and use that in their targeted attacks.

“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,” the report says.

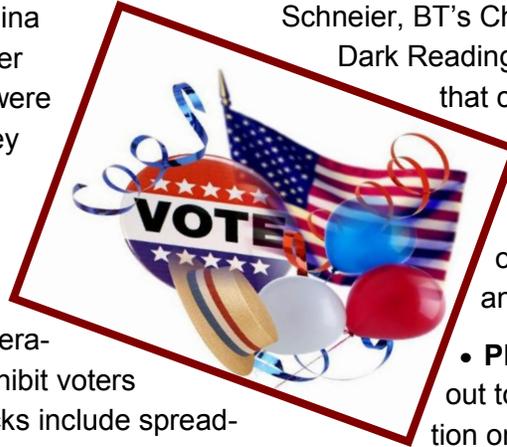
Bruce Schneier, who contributed to the report, says not to expect election officials to do much about these threats: they are still relatively new on the election scene; there's not much they can do about them. “Basically, the moral is that dropping the cost of communication down to free means that both good and

bad communication is much cheaper. We know this is true for commercial email: spam. This is also true for deceptive voting suppression practices,” says Schneier, BT's Chief Technology Security Officer.

Dark Reading summarized the types of tactics that could be deployed online:

- A state election board's **website could be spoofed**, with purposely deceptive information on polling-place locations, times, and voter registration rules.
- **Phishing emails** could be pushed out to voters, offering phony information on polling sites, voter records, voter registration, and voter registration status in an effort to confuse or scare away voters.
- **Pharming emails** could use hijacked domain names such as “Get Out the Vote,” according to the report, as a way to redirect voters to fraudulent sites.
- **Massive attacks** could be launched on voter information sites or voter help hotlines to deny access to the site.
- **“Rumor-mongering”** efforts could be launched that seed fake stories through blogs about election delays or cancellations “due to an emergency.”
- Poll workers could be targeted by **social engineering** tactics that result in delays in poll-location openings.
- A **“Google bomb”** could be set to boost a Web page ranking with phony links.

The EPIC report also makes recommendations to election officials and voters in how to look out for these scams and prevent themselves from falling victim to them.



US Employee Practices Found to be Least Risky!

Shawn Nichols, reporting from San Francisco for VNUNET.COM writes that too many employees are continuing to practice risky behavior, bringing grave risk to their organizations and possibly themselves. The one comforting note about this was that American employees are not the worst transgressors.

He wrote that many employees are continuing to behave in a way that puts company or customer privacy data at risk, according to a study commissioned by Cisco. A survey asked a number of employees in the Americas, Europe, and Asia about their general computing practices and compared them to their organization's IT policies.

Many IT security professionals might be surprised and concerned that potentially risky behavior, such as downloading files for personal use or deliberately modifying system security settings, remains prevalent among many users.

Mr. Nichols states that around 14% of notebook/laptop users deliberately alter the security settings on their company machines. The numbers were highest in China and Brazil, while figures in the UK and US were lower than the average at 9% and 2% respectively. Though US employees may feel good about this, those two percent are still putting their organizations at very grave risk.

Gaining web access was the reason most commonly given among those who had altered security settings. Just over half said that they had altered the settings in order to view a web site which was normally prohibited by company policy. Second on the list was privacy concerns, implying that they felt their activity on the network was private, despite their using work computers and networks. This was cited by 35% of users.

Around a third of the users admitted to allowing a co-worker to use their computer unsupervised, while 13% let a family member access their system.

Unfortunately, IT administrators are not always aware of the risk these employees are imposing on their network and information.

On average, 55% of IT decision makers believed that employees were running unapproved applications on company machines.

However, 24% believe that unapproved programs did not account for any data leaks, while 53% believe that the behavior accounted for less than a quarter of the leaks.

Mr. Nichols also stated that unauthorized access is not a major concern for administrators either. While 40% of IT decision makers have had to deal with employees gaining unauthorized access to a system, 53% reported having to deal with such situations only a few times a year, and 35 per needed to address the issue once a year on average.

With this article in mind, it's refreshing to know that US employees are more aware of their responsibilities on their work computers. Plus, I believe that in the US, IT administrators realize that they need to help raise user awareness while also providing other security tools and policies to protect the network.

State of Idaho employees can refer to their Computer and Internet Use policies in their agencies. Furthermore, the IT Resource Management Council Policies, Standards, and Guidelines provide further information on what an employee should or should not do while protecting the information with which they have been entrusted.

<http://itrmc.idaho.gov/plan&policies.htm>



Office of the CIO, Cyber Security Newsletter

650 W State St
Boise ID 83720
Phone: 208-332-1851
E-mail: terry.pobst-martin@cio.idaho.gov



Links to top Security Websites:

Good websites to surf:

- <http://www.sans.org/>
- <http://www.cert.org/>
- <http://www.msisac.org/>
- <http://csrc.nist.gov/>
- <http://www.issa.org/>
- <http://www.infragard.net/>
- <http://www.ic3.gov/>
- <http://www.securityfocus.com/>
- <http://www.snopes.com/>
- <http://www.nationalterroralert.com/>

**Be a part of the Solution!
Learn your Responsibilities.**

Facebook Malicious-ware Spread by Videos (from F-secure)

F-Secure, a computer security company, revealed that a new Facebook malicious software attack was being spread by videos that had been recommended by “friends” on Facebook.

Facebook users were receiving messages from friends recommending an entertaining or illicit video to watch. Once they clicked on a link, they were redirected to a site which offered a video. It might have looked like this:

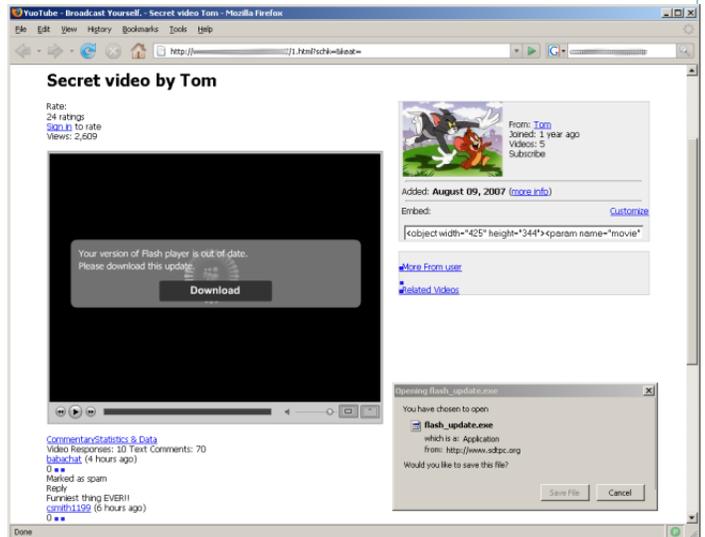


Once they were at this site, they would receive a notification that they needed to update their Adobe Flash Player (or similar program) and they were told to download a file.

As you might expect, no matter how many times they downloaded the file, they did not see a video, but their computer was infected.

The one known worm that was involved in this recent case is known as Net-Worm.Win32.Koobface.bp. or .bm which replicates itself by finding Facebook cookies and posting messages on friends sites so that they will also load the malware.

Facebook is becoming more and more popular among malicious hackers when trying to spread their malicious ware. Remember, once a hacker has any kind of foothold in a computer, you can be assured that they are planning even more malevolent actions against the computer or the information in the computer’s memory.



More Phishing Scams (from Infragard):

The Better Business Bureau warns of a new email scam that is intended to infect your computer with a virus. The scammers are posing as the BBB and are asking you to register for software or to update your information. The scammers pick credible agencies like the BBB to gain trust. On the morning of October 24, the scammers sent out a massive attack to prey on people's trust. The only way the BBB found out about this is that the scammers altered their email address to the real BBB email address. When more than five million emails were undelivered and bounced back to the BBB office, the BBB discovered the scam. The BBB hopes that by warning consumers early about this new scam, they will prevent us from becoming victims.



Don't bury your head in the sand!

Find out more about the security of your information and how to protect your identity!

The next two presentations are scheduled for:

October 31st in the West Conference Room of the JRW Building at 9:00 a.m.

November 12th, in the ITD Auditorium at 9:00 a.m.

Call:

Terry Pobst-Martin with any questions - 332-1851.

The Office of the CIO provides Computer Security Awareness for Employees every month now.

