ONE REALLY GOOD IDEA EVERY DAY
attorneyatwork@

Online Shopping? Five Security Tips

BY DON TULIAO | ATTORNEY AT WORK DAILY DISPATCH

Even if your firm has a policy against it, there's a chance that online shopping is happening in your office – especially during the height of the holidays. Why be concerned? For one, hackers are actively working to compromise any size environment. Two, if you or anyone in your office opens an email or clicks a link to an unsuitable website and the network gets infected, fixing the situation can be costly.

Things to Do to Safeguard Your Data

Here are five tips to help steer clear of cyberattacks. And don't keep these to yourself. Encourage everyone in your firm to take an active role to ensure network security.

1. Beware of spoofed or forged emails. Be extra cautious about emails from unfamiliar sources that make claims about an account or ask you to click on unfamiliar links to take action. Ask yourself, "Why is this company emailing me? Is this organization legit? Does this offer look credible?" Look for misspellings, capitalization mistakes, bad grammar, unprofessional punctuation (such as "!?!") and distorted graphics or backgrounds, which are most likely a cut-and-paste from a legit website.

Be prepared for a slew of fake emails with fantastic offers on merchandise this time of year. Like the old adage goes: "If it's too good to be true, it probably is." If you receive a suspicious email, hover your mouse above the link you're asked to click. This will most likely show you the website URL it's coming from. If it doesn't look right, don't click on it. Delete the email and notify your IT administrator.

2. Search smart. When searching for information or merchandise, stick with the popular search engines such as Google, Bing, Yahoo and Ask. Google has started to include SSL/TLS as a factor in search rankings. This means, in theory, the more "safe" sites will tend to appear first. Any of these web browser plug-ins will notify you if a particular website you visit is considered safe or not:

- WOT (Web of Trust)
- McAfee SiteAdvisor
- Norton Identity Safe

Also consider "sandboxing" your browser, PDF reader and applications to protect against rogue software, spyware and malware by using an isolation program such as Sandboxie.

3. Seek trust indicators when shopping online. Look for websites that are encrypted, meaning that their URL starts with https:// (where the "s" stands for secure). Also look for the lock symbol in front of the https:// — as well as site seals from known security companies, such as McAfee and VeriSign, among others.

4. Avoid sites with risk indicators. Legitimate websites have secure certificates. Some sites have self-signed certificates. Those are the ones hackers use since they don't bother purchasing a legitimate one. When visiting a site with a risk indicator, simply run away! If you feel unsure

of a site and want verification, copy and paste the link into either of the following and it will go through a verification process and show you the results:

- http://safeweb.norton.com/
- http://www.trustedsource.org/

5. Use good password hygiene. Change passwords every 90 days. Make your password easy to remember but hard to guess. Use more than eight characters and mix it up with these variations:

- UPPER and lower case
- Numerals
- Punctuation marks

Don't reuse old passwords, and vary your passwords among sites. To check a password's strength, go to this URL: https://howsecureismypassword.net.

Also, be careful with your answers when setting up your password-challenge questions. Do not use answers that are easily verifiable through social media or searchable public databases. For example, for the question "Which city you were born in?" do not use the actual city as your answer. Instead, use another city that is memorable to you.

Don Tuliao *is a senior system engineer at Innovative Computing Systems. He can be reached at dtuliao@innovativecomp.com. More system security tips can be found at www.innovativecomp.com.*