Agility NETWORKS

e-Newsletter
November 2016

Internet Security Awareness (work and personal): 2016 End of Year Phishing Targets

If you send e-mail, post updates on Facebook, check your bank account balance online, or do most anything that requires the Internet, unfortunately you are at risk of being hacked. Hackers and spammers are always trying to find new ways to trick their victims into clicking a malicious link or downloading malicious software. Among some of the common topics that interest the public are news articles about terrorism, political news, refugee crisis', online dating, celebrity gossip and job offers. This year we had the added bonus of a presidential election going into the holiday season. Well known examples include:

- Links to “news” articles about political propaganda or news articles addressing current events
- Online holiday sales offering great deals
- Holiday fundraisers for the sick/injured/needy

What You Can Do?:

Don’t get suckered in by emotionally charged baits. Instead of clicking the link provided in an email or popup window, use a web browser or search engine to visit the company website instead. If you are donating money, always research the cause and the foundation to make sure they are legitimate before you fall for a sob story. Many hackers even impersonate legitimate, well-known companies to attract their victims, so make sure you are visiting official sites. Use antivirus software that includes web protection and use good web practices when browsing. You can’t control vendor websites, but you do have control of your own PC. So make sure your computer software is up to date. If you happen to use Linux or OSX, don't assume that you are immune either! Here are 5 additional easy tips to protect your life online:

1. Be Aware of What you Share

You don’t have to delete your Facebook or Twitter account, but posting birth dates, graduation years, or your mother’s maiden name --often used to answer security questions to access your accounts online or over the phone-on social-media sites, makes a hacker’s job even easier.

2. Pick a strong password

It can take a hacker only ten minutes to guess a password made up of six lowercase letters. Passwords with uppercase letters, symbols, and numbers (or even using phrases) typically work well.

3. Use 2-step verification

Facebook and Gmail have an optional security feature that, once activated, requires you to enter two passwords- your normal password - plus a code that the companies text to your phone-to access your account. Yes, the added step is an annoyance (aka: a slight inconvenience), but definitely worth the trouble if the alternative is getting hacked!

4. Use Wi-Fi hot spots sparingly

T-Mobile and ATT, the largest providers of free public wireless internet (the kind often available in coffee shops, airports and hotels), don't require encryption of data traveling between laptops and the internet, which means any info (your email password, your bank account balance, etc.…) is vulnerable to hackers. In windows, right click on the wireless icon in the taskbar to turn it off. On a mac, click the wifi icon in the menu bar to turn off wifi.

5. Back up your data

Hackers can delete years' worth of emails, photos, documents and music from your computer in minutes. Protect your digital files! In a nutshell, if at all possible, don't shop or use personal email/social media at work. You could be introducing massive amounts of unnecessary risk to your corporate environment. Downloading games or apps to a company computer is almost always not a good idea, and for good reason! Many are infected with malicious code, even if the application appears to function normally. Use work assets for work. Period. If you have any concerns or questions on how to make your online life (both work and personal) more secure, feel free to reach out to your Agility consultant.

Questions, comments, feature requests? Call us at (877) AGILITY
Would you like to change your subscription? Email 'opt-out' to webmaster@agilitynetworks.com