Internet Security Best Practices - 2014

NAR Information Central - Nov. 2014

Part I:
Internet Chicanery: The Basics

You've probably heard all of the buzzwords related to duplicitous acts and schemes that take place on the web—clones, *phishing*, *malware*, *worms*, *viruses*, and *Trojan horses*. But what you may not know is the difference between each type of activity. In this article, we'll break down the basics of each.

Attack of the clones!
Cloning is perhaps the least dire of the illegal activity that takes place on the Internet. Nonetheless, it certainly can prove distressing. Essentially, the cybercriminal takes a combination of your name, an image of your likeness and perhaps other information personal to you, and creates a new social media profile. One day, you might see your face and name pop up in the "people you might know" bar on Facebook or LinkedIn and feel alarmed, or perhaps a friend sends you a message alerting you to a cloned profile.

Alternately, cybercriminals may set up cloned websites that look almost identical to say, your bank's website, encouraging you to enter personal information. In fact, some scams entail a robocall with a recording that encourages calling back and typing in bank account numbers, or visiting a mock, cloned website.

Phishing for your information and malwaring-up your computer devices
We've all received at least one email from a Nigerian Prince, looking for assistance in a lucrative investment opportunity, or perhaps a "Look at this funny video of you" message from a friend on a social media site. Flattering as such messages may feel, by now we know they are scams. Typically such messages contain malicious "phishing" links that you are encouraged to click on. Once you click on such a link, bad things happen. Malicious software—known as "malware" or "spyware"—is often installed on your computer, recording your every keystroke to garner logins and passwords to all of the sites you frequent. Before you know it, the cybercriminals responsible for the attack suddenly have access to your email, bank accounts, credit cards, and much more. Malware comes in many forms, each form seeking a specific type of malicious action. Viruses, Worms, and Trojan horses are all types of malware.

Worms, and not the garden-friendly kind
Behaving much like bacteria, computer worms are a type of malware that seek to self-replicate, using the infected computer or device as a "host" to spread damage to additional computers and devices. Often they operate under the radar by not altering files on their host computer, but rather using the host computer as a means to access and infect additional computers and devices. Worms operate independently and do not need a human's guidance to replicate and cause damage. Worms often take advantage of holes or weaknesses in software programs; this is why it is vital to keep software programs, such as Microsoft Windows and Adobe Flash, up-to-date ("What is a Computer Worm," n.d.). Worms can cause extensive damage to an entire network of computers.

Outbreak: You've got a virus!

Viruses are also in the malware family and can cause great harm, often rendering computers and devices in a permanent state of disrepair. Through an executable file, viruses alter the existing framework and files on the infected computer or device. Viruses start with one infected file that is transferred and "executed" on one or more computers. Virus files are executed when one downloads an executable file that contains a virus, and then allows his/her computer to run the executable file. Viruses require human interaction in order to propagate.

Trojan horse rampage

For those familiar with Homer's story *The Odyssey*, the concept of a Trojan horse is nothing new. For those not familiar: the story has it that the Greeks built a giant wooden horse, used to conceal armed warriors, and presented it as a "gift" to the City of Troy; whilst the city slept, the warriors crept from the horse and conquered. Not unlike the historical Trojan horse, the computer malware Trojan horse arrives in the form of an enticing website link or useful "software update" request; upon clicking or accepting such requests, the Trojan horse is installed on the computer and begins a series of malicious actions, similar to that of a computer virus.

Conclusion

With all of the above items, ***prevention*** is key. Cisco offers that, "The vast majority [of malicious software] are **installed by some action from a user**, such as clicking an e-mail attachment or downloading a file from the Internet." In our next article, learn the steps to prevent malware from penetrating your computers and mobile devices.

References

What is the difference: Viruses, Worms, Trojans, and Bots?, (*Cisco,* n.d.).

What is a Computer Worm?, (*Symantec*, n.d.).

Internet Security Best Practices - 2014

NAR Information Central - Nov. 2014

Part 2:
How to Prevent Malware Installation and Successful Phishing

Unfortunately, phishing and malware schemes are not going away any time soon—cybercriminals have found such methods far too lucrative to stop. So, we recommend instead focusing on ***prevention***. Cybercrime schemes are in a constant state of change, making it vital to keep up-to-date with the latest best practice tips. Included below you will find several measures that focus on prevention, but keep in mind that on-going prevention requires active engagement in learning about the latest trends.

Please note this guidance is intended for computers and accounts that you personally own. If you are looking to take any of these steps either on a computer or account managed by your company, you may want to consult the IT department first. For example, installing a virus scanner on a computer that already has one can cause that computer to seize up, and can often make a bad situation much worse.

Prevention: Make sure your Firewall is on!
The first step in the line of defense is turning on your computer or mobile device's firewall. Much like the firewalls used in commercial real estate buildings—designed to prevent the spread of fire—computer firewalls seek to prevent hackers from spreading the vicious tricks of their trade (i.e. viruses, worms, and malware). Firewall software is often included in basic computer software packages. For example, firewall software is included in the Windows software suite. Often, upon installation of such software, the firewall is automatically turned on. However, it is always important to double-check that your computer or mobile device's firewall is turned on.

- Why should I turn on my firewall?
  - In the world of Internet security, turning on your computer or device's firewall is the first line of defense. There are many steps to take to increase security; consider turning on the firewall as your first important step.
- How to turn on the firewall for Mac, Mac for Applications, and Windows

Prevention: Password vaults and storage tools
Another tool of prevention is to use an encrypted password vault to store logins and passwords for the various websites and tools that you use. Password values can generate super secure passwords and increase security. Examples of password vaults include 1password, LastPass, or Password Safe (source: New York Times). If you decide to use a password vault, make sure the password to your password vault is extremely tricky, and only use this password once for this particular tool. Never forget this password, either! The password to your vault will be the key to access all of your logins and passwords to other tools.

Another important tool related to prevention is to create extremely tricky passwords, particularly for your most important accounts (credit card, email used to retrieve passwords, bank, and insurance sites). It's time to step into the 21st century and use something more complicated than "*password*" or your pet's name.

When creating passwords: try not to spell out words. Words are easy for hackers to systematically guess using snippets of programing code. Instead perhaps use an anagram—i.e. "How much wood did a wood chuck chuck?"—would be hmwdawcc and then add in some capitals, numbers, and special characters:

→Hmw!daw?cc563#

(source: New York Times - See the New York Times' short video How To Create a Secure Password for more tips).

Prevention: 2-Factor authentication
Along with password vaults and creating secure passwords, consider using 2-factor authentication tools. 2-factor authentication sounds complicated, but the principle is simple: instead of only needing to enter a username and password to log in to a website, 2-factor authentication requires entering an additional piece of information to log in —such as answering a security question. Some websites and tools offer 2-factor authentication as an extra security precaution—take advantage of this option anytime it is offered. Wired explains 2-factor authentication in detail in article Three Essential Steps to Make Yourself More Hack-Proof, (Sept. 5, 2014).

There are also some neat tools that will assist with 2-factor authentication. Google offers a 2-factor authentication app called "Google Authenticator." This tool randomly generates numeric codes that one must enter to log in to sites that enable Google Authenticator. If the app is on your smartphone, and your smartphone is in your possession, you are the only person in the world who would have access to these codes. The only challenge with Google Authenticator is if you lose your phone—you may not be able to get into any of your accounts. However, Google Authenticator provides a list of a one-time verification codes that can be use as backup—so store those codes in a safe place, such as the encrypted password vaults mentioned above.

Prevention: Regular file back-up
It is important to back up computer and mobile devices regularly; either to an external hard drive and/or cloud. This is important because if your computer or mobile device is infected with malware to the point of irreparability, you can install the files from your external hard drive or cloud on a brand new computer or device (granted, your external hard drive has not been infected too and/or the files on your cloud are clean from malware—be wary!). Never plug in an external hard drive to a computer or mobile device that may be infected with malware—the external hard drive functions much like a computer and once infected, can easily spread malware to all computers and mobile devices it comes into contact with.

In some instances, hackers may hold your computer's data hostage, requesting a ransom before returning the files. If you've backed up your files, then you have more options; otherwise, often the only way to get back your data is to pay the ransom (source: NPR).

Prevention: Software updates and malware scans
Another important step in Internet security is regularly running software updates and security software scans. It seems inconvenient when seemingly inundated with update notices for Windows, Adobe, Java, iTunes, and the gamut of

software installed on a computer. However, with the tweak of a few computer settings, it is easy to schedule the updates to install once or twice a week, at the end of the work day or another convenient time. Hackers often exploit weaknesses in software to obtain access to your computer and mobile devices. Often, software updates "patch" these weaknesses, so it is vital to ensure updates are run and installed frequently.

Running updates

- **Updating software on Windows devices**: on a Windows computer, one can click into the "Control Panel" "Windows Update" and find the option to "Check for updates" to see what critical and optional updates are available to install. When in the "Windows Update" menu, one can click on "Change settings" to see when updates are scheduled to install and adjust settings.
- **Updating software on Apple devices**: learn how to turn on and schedule Apple software updates here.
- **Updating software on Apple devices using iOS:** learn how to turn on and schedule updates to Apple iOS devices here.

Security scanning tools

- Microsoft Security Essentials is a free antimalware software package offered by Microsoft, designed to run on Windows XP, Windows Vista and Windows 7. Of course, there are a plethora of security software products on the market and it is up to you to decide which tool(s) suit your needs. CNET offers reviews of many types of software and devices and is a good place to learn about the options. Running a search for antivirus or antimalware returns reviews for a number of tools.

- **Warning**: While it is important to regularly run software updates to make sure all of your computer or mobile device's programs are up-to-date, be wary of Internet pop-ups that require downloading a software in order to view or continue to a website and *__never__* download software from such a website. This is a trick some hackers use to install malware on your computer (Source: NPR). Instead, if you think a particular type of software needs an update, navigate directly to the company associated with that software.

  → Example: if you are told you need to update Adobe Flash Player, then navigate directly to Adobe's website to find the software download. If the software is unfamiliar, research the software first before downloading or installing anything.

Prevention: Suspicious links and personal information on the web

Always proceed with caution when searching the web and clicking on website links, even links found from a Google or search engine search. Be particularly wary of links when using social media and email. We've all seen the messages from hacked friends saying "Look at this funny video of you" or "Ha ha, you've gotta see this." Use your best judgment and if you think a link looks suspicious: don't click it. If you must know where the link goes, then use your mouse to right click and copy the URL, and then paste the URL into a blank Word document so you can see where the URL is actually directing. When in doubt, send a new email to that friend or give her/him a call to make sure it is legitimate. You can also use the words used in the email and link in an Internet search to see if you can find a link to a legitimate and trusted website—perhaps others have posted warnings about such messages—just be sure you paste the text into a search engine box (e.g. Google or Bing), and not the web address URL bar ! If your bank or another trusted organization sends you an alert asking you to update your account information, never click the link in the email. Instead, navigate directly to the bank's website using a trusted URL web address, making sure there is an "s" in the

website address, as in https:// before logging in.

It is also wise to be wary of putting your email address up on a website. Hackers and spammers often use web crawlers or other pieces of computer programming code to methodically comb the web, looking for email addresses and other personal information. If your email address is easy to grab on the web, you will likely see an increase in spam and your email address may be shared with additional parties. To get around web crawlers, many companies and professionals use web forms (often with a "captcha" image for extra security) that prospective clients fill out in order to get in touch with you.

Prevention: Encrypting email and Internet activity

Encrypting your emails adds an extra layer of prevention in guarding your personal information. Encrypting renders emails unreadable as they travel from server-to-server, making them readable again once they reach the intended email recipient's inbox. Encrypting can be as simple as making sure that websites you use include the "s" as in https:// which denotes the use of a "Secure Socket Layer" (SSL) to protect information entered and transferred on the website. However, when using a non-web based, desktop client to send emails (such as Microsoft Outlook), encryption can entail some additional steps. PC World offers a great article, "How to encrypt your email" (2012) which details the steps one can take and includes this insight:

"To secure your email effectively, you should encrypt three things: the connection from your email provider; your actual email messages; and your stored, cached, or archived email messages."

Additional resources for learning about encryption include:

- Encrypting iOS
- Encrypting BlackBerry
- Encrypting Windows Phones
- Encrypting Samsung Devices

Prevention: Extra security measures

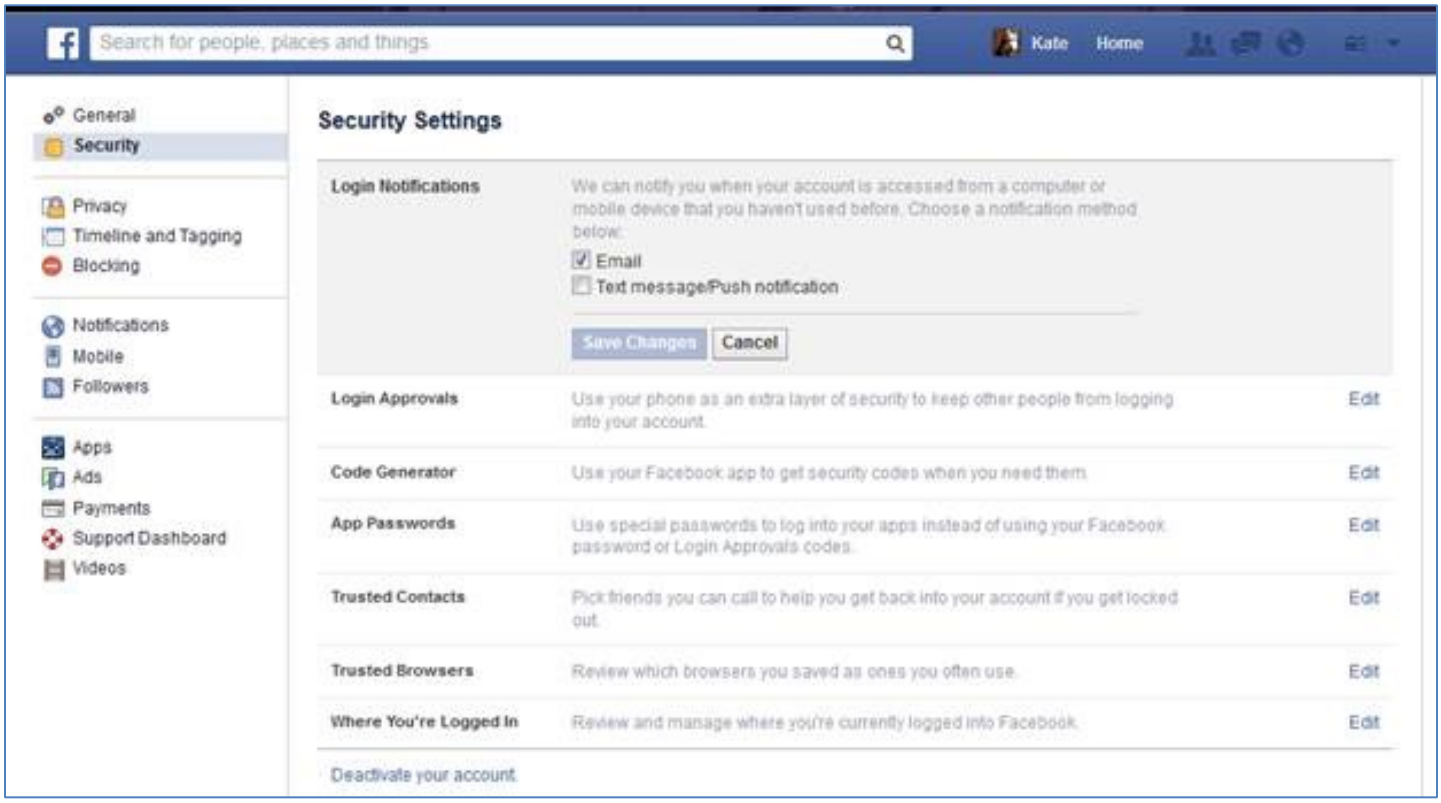
There are a few extra security precautions or "best practices" one can pursue, to minimize the risk of encountering malware. These include:

- On social media: don't *friend*, *link*, or *follow* people you don't know. This is particularly important on sites like LinkedIn and Facebook, as it is easy for someone to gain access to a lot of personal information about you that can easily be exploited. This information can be used to create new "mock" or clone profile to spam your friends, or used in conjunction with other information about you for identify theft.

- When registering with a website that offers extra security measures, such as security questions or 2-factor authentication: use it. Always opt to add additional security measures if a website offers it. For example, in Facebook's security settings, one can opt to receive an email any time someone logs in to your account from an unknown device:

Internet Security Best Practices - 2014

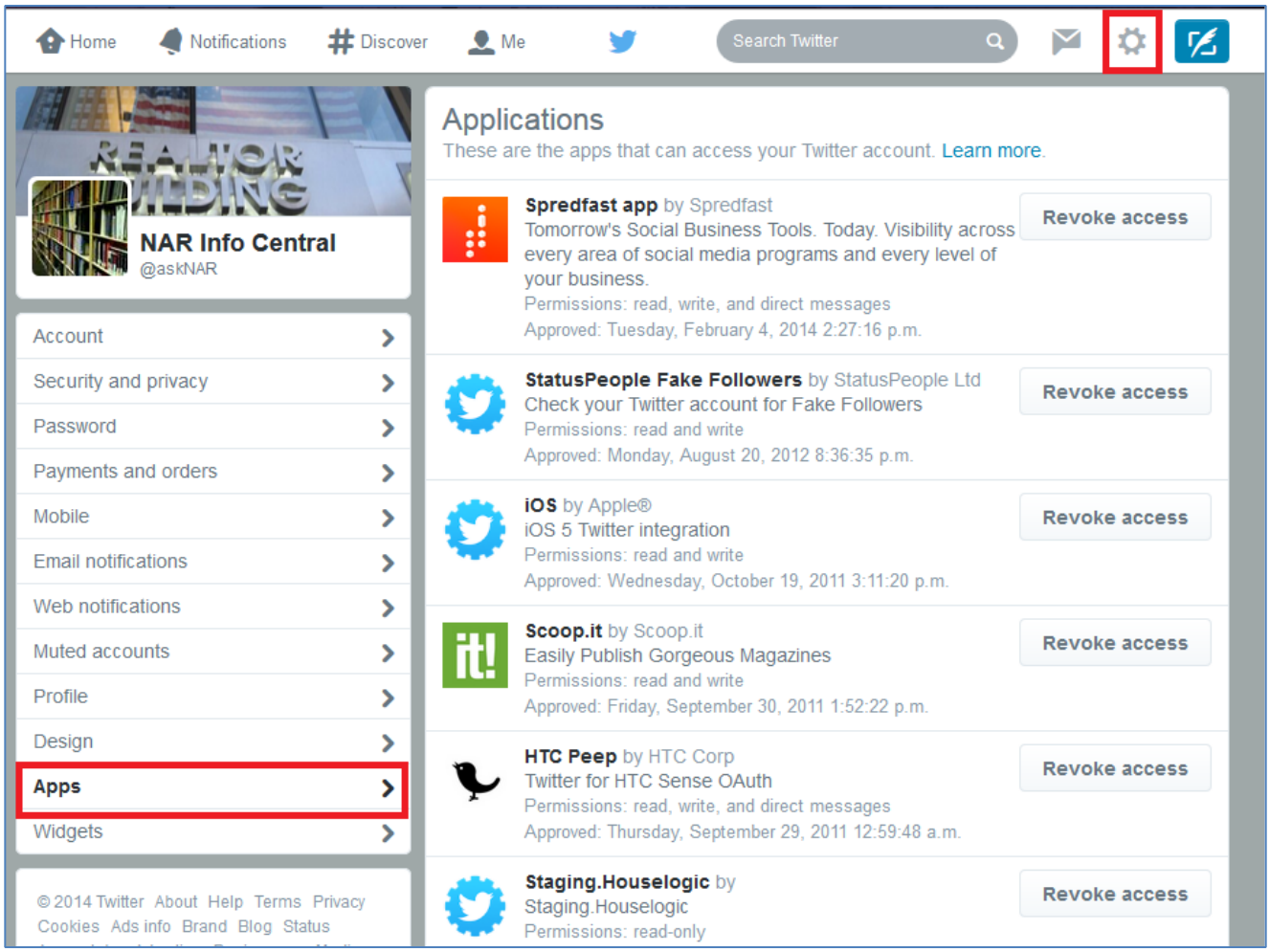
NAR Information Central - Nov. 2014



Prevention: Monitor

Another tool of prevention is *monitoring*. This entails action on your part. It is important to regularly monitor your bank and credit card statements to make sure no charges are unaccounted for, and to make sure you only use your credit card with trusted vendors, both in-person and online. Additionally, be sure to monitor your email to make sure you are familiar with any/all email delivery rules and filters tied to your account, and delete any that look suspicious. Email rules and filters allow for auto-forwarding messages to a different email inbox or specific folder. If you're not familiar email filters and rules, search your email provider's help documents to learn more. Some examples include Gmail, Windows, and Yahoo!. It is also wise to check your sent mail to make sure it contains only messages you have written and sent yourself.

Monitor apps tied to your social media accounts—such as Twitter and Facebook—to make sure that only apps you've approved are listed, and delete any app approvals that look suspicious. Additionally, always read terms of use before approving third party apps. It is important to make sure you know what you are agreeing to before you download or approve an app. For example, in the account settings menu on Twitter, there is an option to view all of the apps you've approved:



Prevention: Lock your wireless network, don't use unsecure wireless networks

Often it is tempting to take advantage of free wireless networks found in public places. However, when considering the use of an unsecured wireless network, you should always ask yourself, "Is a few minutes of free and unfettered fun worth the risk of losing control over my identity and computer/mobile devices?" If you're not sold on this idea, take a gander at PC World writer Eric Geier's article on what he found when snooping on a public wifi network.

Prevention: Throw-away email address

These days, registration and a login is required to do most anything on the web. You may find it helpful to create a "throw-away" email address that can be used when registering and creating accounts with non-commerce websites,

such as for news agencies and social media sites (and any other websites that do not require the use of your credit and bank numbers). Be sure to keep this email account separate and distinct from the email account tied to your e-Commerce transactions.

Prevention: Personal information

Another important step in prevention is to not share your personal information when it is not required. Do not share personal information when registering with a website, particularly if it is not required (source: CNN). Typically, if a field is required you will see an asterisk * next to it, denoting it is required; if you don't see an asterisk *, then leave the field blank.

Prevention: Keep yourself up-to-date!

Internet crime is not likely to go away and criminals will always find new ways to get at your data, so arm yourself with up-to-date information on privacy and security and stay apprised of changes and new developments. When you learn of new changes and developments, always respond accordingly to keep your data and Internet activities secure.

Prevention: How to prevent cloning

Employing good social media privacy and security practices is the first step in preventing cloning. When you "friend" someone, you instantly give them access to a plethora of information about you—more images, more personal details, more information on your everyday activities. This makes it even easier for the cybercriminal to create a brand new clone of your profile and take advantage of your good reputation to spam your friends and family, or engage in other malicious activities. The moral of the story: don't "friend" or "connect" with someone you do not know. Flattering as such requests may feel, make sure you actually know someone before you accept any requests. And, if you are already friends with someone and you get another friend request from them: be wary, it may be a clone; contact that person first, before accepting any friend/connection requests.

If you keep your social media profile information "unlocked" and accessible to all, you increase your vulnerability to cloning. When your account is unlocked, cybercriminals have access to all the information they need to clone your social media profiles and even store your personal information for other dubious activities. The moral of the story: make sure to update your social media profile settings to only share your information with your friends and connections. Social media sites are constantly changing their privacy and security practices, so unfortunately there are no set steps by which to "lock down" your social media profiles. However, it is suggested that you regularly (i.e. every couple of months) check out privacy and security settings on your social media accounts to ensure you know exactly what information is accessible to the public.

For example, at this time one can log into Facebook, go to her/his own personal profile page, and in the "Cover photo" image, at bottom right, click on the "..." ellipses, then click "View as..." to see what the "Public" sees. At most, we recommend only showing the public your profile photo—everything else, including information about you, where you work, and your photos should all be designated as private, and accessible ONLY to friends. We do not even recommend allowing "friends of friends" to see your content.

You can take things one step further, too. For example, under Facebook's *Settings* you can set up your profile so that it does not display in a Facebook website search—meaning only your current friends can look you up using your email address and phone number; you can even opt out of search engines linking to your timeline. Keep in mind that these settings are likely to change as social media sites add new features. Social media sites often benefit, financially, when your information is public—so often, their default is to make your information public. It is on you to keep an eye on your settings and update when new features are added.

Internet Security Best Practices - 2014

NAR Information Central - Nov. 2014

Part 3:
What to do when you've been hacked or clicked on a suspicious link

Please note this guidance is intended for computers and accounts that you personally own. If you are looking to take any of these steps either on a computer or account managed by your company, you may want to consult the IT department first. For example, installing a virus scanner on a computer that already has one can cause that computer to seize up, and can often make a bad situation much worse.

Please also note that, should a computer or mobile device become infected, it is wise to consult with an expert to ensure malware is completely removed and that it is safe to continue using the device.

What to do when you find a clone

It is alarming when you find that someone has created a profile, identical to yours, with an image of your likeness and your name. Each social media site has their own terms and conditions by which you can report a clone and request its removal. You might be asked to scan and email (or fax) in a copy of your driver's license, to prove you are who you purport to be. Since reporting requirements are always changing, the best thing to do is to navigate to the social media site's Help section and search for "cloning help" or "cloning" to determine the next steps.

What to do if you click a sketchy link or malware is installed on your computer

1. Abort mission immediately!! As soon as you know or feel like you've clicked a bad link, immediately disconnect your mobile device or computer from the Internet. This will temporarily prevent hackers from accessing your computer or device. It will also prevent your computer or device from communicating with other devices in your network and causing further damage.

2. Don't plug or connect any other devices to the infected device. This will cause further damage by opening up other devices to the virus, worm, or malware.

3. Use an alternate secure device or computer, on an alternate Internet network or wireless connection, to change passwords to the affected services and/or your most vulnerable services/sites (i.e. your bank, insurance providers, email accounts, password vault). If you use the same password for multiple services: shame on you! Change the passwords to any other services that use that same password, too. DO NOT change passwords on the infected device before running a virus scan (source: MSFT). Hackers may have access to your computer/device and thus the ability to monitor your every move.

4. Purchase or download trusted anti-virus, anti-phishing, anti-spyware for your device and run it. Try not to connect this device to the Internet, especially if you've interrupted any virus-download process by disconnecting the Internet (perhaps download trusted software to a different device and use a thumb drive or cd to transfer the software to the infected device).

5. Check for backdoors—look through your email rules to make sure the hackers didn't set up email forwarding, and update your security questions to make sure they were not changed.

6. Monitor! Monitor all accounts, check for new email rules, account security changes, and any strange or unauthorized charges on credit cards and bank statements.

7. Think about connections—the account or device that was hacked: what other tools/services tie into or associate with that account? Check and monitor those for vulnerabilities too!

8. De-authorize all apps tied to your smartphone, tablet, and social media accounts—apps interrelate and authenticate—so de-authorize these relationships and then re-add them later.

9. Identity and credit monitoring—keep an eye on your credit report and consider setting up identity and credit report monitoring for at least a few months to be alerted to any suspicious activity.

10. Let your communities/networks know what happened—tell them not to click suspicious links in emails and posts from you in the interim or to confirm with you first before clicking.

11. Some Internet security experts suggest that one should not use a previously infected device to access vulnerable information—like bank, insurance, and credit sites—even after the infected device has received an anti-virus treatment. It's up to you to decide upon an infected device's trustworthiness.

12. Be sure to take good notes of everything that happened prior to the security breach—try to remember how you arrived at a particular website, what links you clicked, what pop-ups or dialog boxes you saw, and any downloads you agreed to. This will prove helpful should you need to consult with a computer expert.

13. Consider consulting with an expert. Find a credible and trustworthy, licensed, bonded and insured, computer expert to review your computer and/or devices to ensure the malware is completely removed. Malware can prove tricky to remove and often operates under the radar.

References

What is the Difference: Viruses, Worms, Trojans, and Bots?, (CISCO, n.d.)

What is a Computer Worm?, (*Symantec*, n.d.).

What to do after you've been hacked, (*Wired*, Mar. 5, 2013).

What to do when you've been hacked, (*PC Magazine*, Mar. 6, 2014).

My account has been hacked, (*Microsoft Windows*, n.d.).

11 Sure Signs You've Been Hacked