A Month of Tips for Cyber Security Awareness Month

Date	Tweet	Tip
1-Oct	Real-world warnings keep you safe online: Don't trust candy from strangers. If it sounds too good to be true, it probably is!	**Real-world warnings keep you safe online** Like the real world, technology and the internet present dangers as well as benefits. Just as you take precautions to protect yourself in the real world, you need to take precautions to protect yourself online. • Don't trust candy from strangers — Anyone can publish information online, so before accepting a statement as fact or taking action, verify that the source is reliable. It is also easy for attackers to "spoof" email addresses, so verify that an email is legitimate before opening an unexpected email attachment or responding to a request for personal information. • If it sounds too good to be true, it probably is — Sorry, but there aren't any wealthy strangers desperate to send you money, that stock tip is not actually guaranteed, and you haven't won a lottery that you didn't enter.
2-Oct	Treat your personal information like cash. Don't hand it out to just anyone. Verify that requests are legitimate.	**Treat your personal information like cash** Don't hand it out to just anyone who asks. Your Social Security number, credit card numbers, and bank account numbers can be used to steal your money or open new accounts in your name. So every time you are asked for your personal information — whether in a web form, an email, a text, or a phone message — think about whether you can really trust the request. In an effort to steal your information, scammers will do everything they can to appear trustworthy. Learn more about scammers who phish for your personal information.

Date	Tweet	Tip
3-Oct	Use cloud services carefully. Know your data's security needs. Read the service's terms of use and privacy policy.	**When online, free isn't always free** There are a lot of free services online these days. You can store pictures "in the cloud," develop documents, send email, and connect people. And it doesn't cost you a single penny. But free isn't always free. Some services want to get you hooked so they can then start charging you. Some services want you as a customer so the service looks attractive to venture capitalists or to larger companies. Many "free" services sell information about you — your likes, hobbies, salary, family members, friends, location, profession, purchase and viewing history, and other demographics — to advertisers to make money. Be aware of what information you're providing online. Read websites' privacy policies and terms of use. Don't post information that could be exploited by a bad guy or that you don't want made public. Don't store unencrypted sensitive information in the cloud. You don't know with whom you're sharing the cloud!
4-Oct	T/F: It's okay to just throw away my old electronics? See the answer on Monday.	
5-Oct Sa	"There is no reason anyone would want a computer in their home." — Ken Olson, president and founder of Digital Equipment Corp, 1977	
6-Oct Su	"I think there is a world market for maybe five computers." — Thomas Watson, chairman of IBM, 1943	

Date	Tweet	Tip
7-Oct	Safely dispose of old computers. Physically destroy old hard drives or wipe them with a special program.	**Safely dispose of old computers** When you get rid of sensitive paper documents, it's a good idea to shred or burn them to help protect your privacy and prevent identity theft. Similarly, it's important to erase your personal information from old computers before you dispose of them. Simply reformatting a disk or reinstalling the operating system does not guarantee the old data is unreadable. Physically destroy the hard drive using a hammer, for example, or use a special "wipe" program. These programs, such as Active@ KillDisk and Softpedia DP Wiper, are free and meet government security standards. Some device refurbishers will also safely dispose of old electronics and securely wipe your data. Learn more: Apple Recycling Program Microsoft Refurbisher
8-Oct	Keep your mobile device safe. Put a password on it and don't leave it unattended.	**Secure your mobile device** Mobile devices are small, go with you everywhere, and contain your life. Remember physical security. Do not leave your device unattended in public or easily accessible areas. Keep software up to date. If the vendor releases updates for the software operating your device, install them as soon as possible. Installing them will prevent attackers from being able to take advantage of known problems or vulnerabilities. Use strong passwords. Choose devices that allow you to protect your information with passwords. Select passwords that will be difficult for thieves to guess, and use different passwords for different programs and devices. Do not choose options that allow your device to remember your passwords.

Date	Tweet	Tip
9-Oct	Verify links before clicking. Use a tool like LongURL to scan a shortlink on Twitter and Facebook to ensure it goes to the expected site.	**Check where a link goes before clicking** With a mouse, hover over the link. The full URL of the link's destination displays in the lower corner of your browser. You can also use a tool like LongURL to scan shortlinks on Twitter and Facebook to ensure they go to the expected site. Some URL shorteners give you the option of previewing the true destination. For example, if you have a bit.ly URL, simply add a "+" to the end of the URL to see the true destination, like this: http://bit.ly/10hVtvV+
10-Oct	Antivirus software really is important. Keep it running and up-to-date. Get an AV app for your smartphone too.	**Understanding AV software** Anti-virus software scans files for certain patterns or signatures of known viruses. Virus authors continuously release new and updated viruses, which is why it's important to always have the latest AV version installed on your computer. Set your AV software to scan your system automatically. And remember to manually scan files you get before opening them. These include files you download from the Internet, email attachments, and files on USB drives and other media.
11-Oct	What is rogue AV software? See the answer on Monday.	
12-Oct Sa	Law of Gravity: Any tool, nut, bolt, screw, when dropped, will roll to the least accessible corner.	
13-Oct Su	Law of the Result: When you try to prove to someone that a machine won't work, it will.	

Date	Tweet	Tip
14-Oct	Rogue AV is fake antivirus software that may actually infect your PC or steal your credit card info. Take the Real vs. Rogue quiz.	**Beware of rogue AV software** Rogue software or "scareware" is fake antivirus or security software. Bad guys usually try to get you to install it by generating a pop-up window as you surf the web. The "updates" or "alerts" in the pop-up windows call for you to take some sort of action, such as clicking to install the software, accept recommended updates, or remove unwanted viruses or spyware. When you click, the rogue security software downloads to your computer. Take Microsoft's Real vs. Rogue quiz to help you tell if a security warning is from your real antivirus software or from rogue security.
15-Oct	Security Myth: I don't have anything a hacker would want. Hackers want your personal info, money, and control of your devices.	**Common Security Myth: I don't have anything a hacker would want** Yes, you do. Hackers want to control your PC to send spam, distribute malware, or help launch a denial of service attack. Hackers want your identity to use for identity theft and fraud. And hackers want your money. Most attacks are automated. Hackers simply seek out and compromise all vulnerable systems.
16-Oct	Security Myth: Security is a concern only if I use Microsoft Windows. ALL software has bugs that hackers can exploit.	**Security Myth: Security is a concern only if I use Microsoft Windows** All software has vulnerabilities and flaws that bad guys can take advantage of, including Mac operating systems, Linux, Chrome, and Adobe Reader. That's why it's so important to apply security patches. Microsoft is the biggest target for hackers because most people use it. Android smartphones are a huge target too, for the same reason.
17-Oct	Security Myth: I will be safe as long as I don't surf porn sites. A hacker can use a site's bugs to make even reputable sites bad.	**Security Myth: I will be safe as long as I don't go to certain types of sites** While any site can be compromised, you should stick with reputable online stores, news, and entertainment sites. Porn, gambling, hacker, and "free" sites are more likely to be malicious. For example, adding the word "free" to searches increases the risk pulling up malicious sites. Remember to look at the status bar at the bottom of your browser before clicking a link to make sure you are going to the site you click.

Date	Tweet	Tip
18-Oct	T/F: It's okay if I'm being monitored — I'm not doing wrong. See the answer on Monday.	
19-Oct Sa	The secret to life. Is contained in this Haiku. Oops, ran out of room. Haiku by Dan from Memphis, TN	
20-Oct Su	Don't run with scissors.	
21-Oct	Privacy is a basic human need, impacts your safety and even the prices you pay. Read sites' privacy policies before giving your info.	**Privacy Myth: It's okay if I'm being monitored — I'm not doing anything wrong** Privacy is the state of being free from unsanctioned intrusion, or the right to be "left alone." It concerns information about you that's collected, used, disclosed, and retained. Privacy is a basic human need. You may not be doing anything wrong, but would you still express yourself freely if you know that you're being monitored? You may also have to pay more for goods and services based on your profile. A lack of privacy may also affect your personal safety if bad guys know where you are. For example, if you post on your Facebook page that you're on vacation for the week, bad guys may rob your home. Then there's the "ick" factor. Who wants to be monitored and tracked?
22-Oct	Pick an anonymous name for your home network and change the default passwords.	**Secure your home network** If your home network is named "John Smith's home" or "Apt 2B," then everybody knows which network to hack into. Pick a generic, anonymous name. Make sure you change all passwords that come with your network components. Those passwords are generally written in user manuals, which are posted online for all to see.
23-Oct	Does a thief or stalker know where you are? Don't "check in," post, or advertise your location.	**Don't advertise that you are away from home** When you post that you're on vacation, or when you "check in" to your favorite meeting place, that tells others not only where you are, but also that you're not home. Your friends aren't the only ones who'd like to know where you are. Thieves and stalkers do to. So do marketers, but they don't usually pose a risk to your physical safety. Resist the urge to tell all!

Date	Tweet	Tip
24-Oct	Is that app giving away your privacy? Always check the access that an app wants. Don't install apps that want excessive permissions.	**Is that app giving away your privacy?** Be careful when you install apps on your mobile device. Many apps want more permissions than actually needed for their function. For example, some flashlight apps want access to your contacts. Why? Usually for marketing purposes to build a better profile on you and your friends. Don't install apps that require excessive permissions. Also, always install apps from a trusted source. Install apps from the trusted App Store or Marketplace. This helps ensure the app isn't fake or malicious.
25-Oct	For some, I'm automatic. But most forget me. Then cry when I'm needed. What am I? See the answer on Monday.	
26-Oct Sa	Bugs and viruses. Incompetent end users. Job security. Haiku by Janice in Edmond, OK	
27-Oct Su	If you spend more on coffee than on IT security, you will be hacked. What's more, you deserve to be hacked. — Richard Clarke	
28-Oct	Have a backup plan. Use a cloud service or save your data to disk or external drive. But make sure to back up your data.	**Have a backup plan** Since your information could be lost or compromised (due to an equipment malfunction, an error, or virus), make regular backups of your information. There are many cloud services that offer backups, and you can schedule automatic backups. Backups also help you identify what has been changed or lost. If your computer has been infected, it is important to remove the infection before resuming your work. Save some older backups, because if your computer gets infected, some of your backups may also be compromised.

Date	Tweet	Tip
29-Oct	Patch your systems. Vendors issue security patches. Install them to protect your devices.	**Patch your systems.** In general, you have to click on something to get a computer virus. But you don't have to do anything to get a worm. A worm is a type of malicious software that takes advantage of a software vulnerability or bug. Worms search the internet for vulnerable devices and then infect them. When vendors become aware of a vulnerability or bug, they issue fix it with a security patch. Prevent worm infections — keep your systems patched and up-to-date.
30-Oct	Don't click! Got an email about some sensational news story or photo? It's probably a trick to get you to click.	**Stop. Think. Click.** Bad guys often use current news, sensational topics, and promises of shocking or sexy photos and video to get you to click on malicious links. Don't fall for their tricks. Stop and think before you click.
31-Oct	Learn more. And remember, as Abraham Lincoln said, "Don't believe everything you read on the Internet."	We hope you enjoyed this month of tips. Learn more. And remember, as Abraham Lincoln said, "Don't believe everything you read on the Internet." Learn more at phoenix.gov/infosec.