

National Cybersecurity Awareness Month



OCTOBER 2019

WEEK 1

Protecting Your Information and Devices

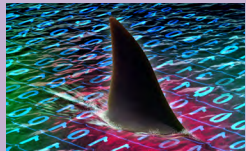
The Internet of Things

Technology has made our lives easier in so many ways. We can write more quickly, enjoy our favorite movies or music, anytime, anywhere, and speak to people in other countries almost instantaneously. Doctors can even use the Internet to perform surgery from hundreds of miles' distance from the patient.

What is Network Security?

In its [Security Tip \(ST15-002\)](#), the US Department of Homeland Security defines home network security in part as "...the protection of a network that connects devices to each other and to the Internet within a home..."

It's so convenient to be able to start your dinner or your car, unlock your doors or turn on your lights, start a load of laundry, or ask the refrigerator what you need to shop for on the way home, all at the tip of a finger; however, all that convenience provides means for malicious actors to steal our information, our sense of security, and our very identities. Online crime is the fastest-growing crime in the US.



In order to navigate the shark-infested waters of our technology-based society, users of that technology need to be aware of the risks that their devices present and how to secure those devices and the information that they process.

What are the Risks?

If a malicious actor manages to hack into a single one of your devices, it might allow them to steal your identity and open up all your other devices to malicious activity. This could mean:

- Clearing out your bank account.
- Opening credit cards, taking out loans, or running up medical bills in your name.
- Using your network to access illicit websites.
- Hacking into your social media accounts to phish your contacts.

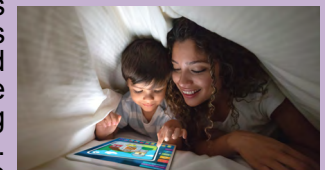


The Deep Web

The Deep Web, also known as the Dark Web or the Invisible Web, contains approximately 95% of www content. This content cannot be indexed by search engines like Google and Bing and is difficult to navigate. Early developers of this peer-to-peer, heavily encrypted system, aimed to allow Internet users to access sites without leaving a browsing history or personal information that others could exploit for everything from targeted advertising to stealing identities. A criminal can use a stolen identity as cover while performing malicious activities like medical or mortgage fraud, selling illicit drugs, or trafficking child porn. As tempting as it may be to shield your online activity from advertisers, the Deep Web exposes users to more dangers than it protects them from, and may land them on the FBI watch list.

Teach Your Children Well

Remember you can use your devices to help keep your children safe online. Children are the fastest-growing group of victims of online crime. Websites such as [us-cert.gov](#) and [staysafeonline.org](#) have great tips for keeping your children safe online. The [www.cynja.com](#) site provides an age-appropriate, safe space for kids that includes activity reports for parents, as well as engaging graphic novels that teach kids about online safety. The KidzSearch app filters Google searches to remove inappropriate content and unsafe sites.



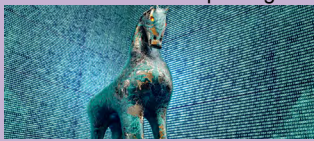
Many apps track your child's location or screen time, and allow you to access that information using your computer or smart phone. Others monitor their social media usage or limit the times when they are allowed to be online.

Being aware of what they are doing online and teaching them safe online habits is your best means of protecting your children from online crooks:

- Talk to your children about online safety, like not talking to strangers or giving out personal information.
- Keep Internet-capable devices where you can see what your children are doing.
- Use device- and app-provided parental controls.
- Set reasonable time and usage limits.

National Cybersecurity Awareness Month



Do This	Here's Why
Keep your software updated.	Software companies release patches to address vulnerabilities that malicious actors can exploit.
Use encryption.	Check your device's security settings to determine whether they offer encryption capabilities. Encryption provides an additional layer of protection for your device and your data while it is in transit. If your device doesn't automatically encrypt, you can use an encryption program.
Use an anti-malware package. 	These packages can protect your devices from viruses, adware, spyware, worms, ransomware, rootkits (malware that allows others to gain administrator access to your device while leaving little to no evidence of its existence), keystroke loggers, and exploits (which can install on your device without your ever having clicked on a link). They are not infallible, but they generally have the most current information on existing malware. Note that although Kaspersky anti-malware software consistently receives excellent reviews, it is illegal to use it on government equipment by order of the Department of Homeland Security due to the company's Russian ownership and association with the Russian government.
Use a password manager that is protected with a strong password.	Password managers create and maintain unique, strong passwords for every site you visit, protecting your data on other sites if one is ever breached. You need only remember the password for the password manager itself.
Change your default passwords immediately and all passwords regularly.	Many password managers do this for you, since they protect access to your data on other sites in case of a breach. Do not reuse passwords. If a site on which you use a password is breached, anywhere else you use it becomes vulnerable.
Be cynical.	Don't follow links that don't provide context, or are sent to you by entities you don't know or haven't verified. If an email, voicemail, or text message says that you need to act on something right away, use a means other than an included link to verify that the action is necessary.
Limit physical access to your devices.	This protects you from those who would add malware or steal your data. This includes being aware of your surroundings and ensuring that you don't enter any sensitive data like a PIN-code where others can see it.
Add two-factor verification.	Although not 100% secure, requiring a telephone or other device that you have in your possession to verify your identity makes it more difficult for malicious actors to access your data and devices.
Add PIN-code protection.	Many devices allow you to create a code that must be entered to access a device, preventing the average person from accessing the data on a lost or stolen device. The longer the code is, the more secure it is.
Set auto-lock for no more than 15 minutes.	This protects you if you walk away from your device (or if someone causes it to walk away from you).
Install a Virtual Private Network (VPN) when not on your private network.	A VPN creates a secure, encrypted connection between you and your service provider. It prevents malicious actors from getting your data using false "public" Wi-Fi accounts and shields your browsing from prying eyes. It can even make you appear to be in some place other than where you are, allowing you to access region-specific content.
Use a device locator and remote wipe capabilities.	If your device is ever lost or stolen, a device locator can help you find out where it is, frequently to within feet. Remote wipe capabilities allow you to delete data from a device even when it's not in your possession, as long as its power is on.
Back up the data on your device.	This allows you to restore your data if your device is lost or stolen, or if you are the victim of a ransomware attack.
Use dedicated email addresses and keep them to yourself.	Using unique and separate email addresses that are not associated with your name for different kinds of online activity such as banking, social media, and shopping provide another layer of protection for your data. If you keep that address information to yourself, you further reduce the chance that a malicious actor can gain access to your data.
Control and delete third-party account connections.	When apps ask for access to your mail, contacts, etc., consider why they would need that information and deny them if they seem unnecessary. Delete the app once you've finished using it to reduce risk to both you and your contacts.
Protect your password re-sets.	When possible, select a setting that requires personal information from you to re-set a password so that it's more difficult for someone else to spoof your identity to access your accounts.
Check your account activity and close accounts you're not using.	Most social media sites let you check your recent activity. Doing this check regularly lets you know whether someone else is using your account. Inactive accounts may provide information that hackers can use to gain access to your active accounts.
Use apps only from well-known companies.	Applications from well-established companies are more likely to have security as a high priority in their development and to have regular security patches available.
Stay informed.	Keeping up with tech news informs you of the latest threats and breaches and how to deal with them, to help you keep ahead of the hackers.
Watch what you share online.	The more personal information you share online, the more chances you give for hackers to access your accounts. Don't post anything that you wouldn't want a stranger to know.

National Cybersecurity Awareness Month



The 20 Most Used Passwords

Password	Times Found in a 2018 Breach
123456	23.2m
123456789	7.7m
qwerty	3.8m
password	3.6m
1111111	3.1m
12345678	2.9m
abc123	2.8m
1234567	2.5m
password1	2.4m
12345	2.3m
1234567890	2.2m
123123	2.2 m
000000	1.9m
lloveyou	1.6m
1234	1.3m
1q2w3e4r5t	1.2m
Qwertyuiop	1.1m
123	1.02m
Monkey	980,209
Dragon	968,625

Passwords Provide Protection

The easiest way for hackers to access data is through breaking common or weak passwords. The UK's National Cyber Security Center (NCSC) 2019 global breach analysis provides a list of the most common passwords found in data breaches. The most recent found that 23.2 million of those hacked worldwide used the password 123456. The 20 most common passwords revealed by data breaches are shown on the left. As many as 100,000 are available to view online at <https://www.ncsc.gov.uk/static-assets/documents/PwnedPasswordTop100k.txt>.

Troy Hunt, one of the world's most renown cybersecurity specialists, has created a safe web site at <https://haveibeenpwned.com/> that allows you to enter your email address(es) and password(s) to see whether they have shown up in any known breaches.

The single most important thing you can do to protect your devices is to use a unique, strong password for each site you visit. Whereas most cybersecurity experts recommend using a commercial password manager to do this, it's not always feasible and it's a good idea to know how to create a strong password.

The best way to make a strong password or pass phrase is debated in the cybersecurity community, but factions agree on a few main elements. First, the longer a password is, the harder it is to break by "brute force," which is trying all combinations of possibilities to determine the correct one. Second, you should avoid using a single word that can be found in a dictionary. Hackers have tools that look for those, no matter how long the word or whether it contains numbers and special characters. Three common methods of generating strong passwords manually are:

- **The Pass Phrase method (also known as the XKCD method):** It consists of using four random common words. The example used in the XKCD comic is CorrectHorseBatteryStaple. This method works best if the words are truly random, which is generally difficult for humans to accomplish. You can make this stronger by adding numbers and/or special characters in and/or between the words or by using dice and a random word generator like <http://world.std.com/~reinhold/diceware.html>.
- **The Bruce Schneier method:** Combine a personally memorable sentence with some personally memorable tricks to modify that sentence into a lengthy password. One example is "When I was seven, my sister threw my stuffed rabbit in the toilet," giving you the password **Wlw7,mstmsr!tt.**
- **The Person-Action-Object (PAO) Method:** Computer scientists at Carnegie-Mellon University recommend the PAO method for creating secure, memorable passwords. The method was popularized in Joshua Foer's 2011 book [Moonwalking with Einstein](#). Create a PAO password using these steps:
 1. Pick a memorable place, such as "The Empire State Building."
 2. Pick a familiar or memorable person, like "Buffy the Vampire Slayer."
 3. Imagine a random action relating the two, like "flambéing a cherries jubilee."
 4. Now combine these into a mini-story: "Buffy the Vampire Slayer flambéed a cherries jubilee on top of the Empire State Building." The images and situation this story describe become the mnemonic device that helps you remember your password.
 5. Finally, select letters from the mini-story to create a password, e.g., **BUFFtVSflb@cj0t0tESB.**



National Cybersecurity Awareness Month

 National Cybersecurity
Awareness Month



T	G	S	S	E	C	C	A	T	I	M	I	L	K	C	Q	M	Y
P	S	A	H	E	S	A	R	H	P	S	S	A	P	H	P	K	P
A	T	R	V	E	R	I	F	I	C	A	T	I	O	N	S	C	A
S	A	D	E	V	I	C	E	S	N	P	B	A	L	T	B	O	R
S	Y	M	D	T	B	S	F	E	I	E	K	I	L	N	I	L	E
W	I	H	E	C	C	O	M	N	N	C	M	U	P	D	I	O	N
O	N	C	E	U	A	A	C	C	C	I	A	V	E	L	S	T	T
R	F	A	P	P	I	O	R	S	T	F	J	N	S	S	P	U	A
D	O	E	W	L	D	Y	R	A	E	U	T	K	T	F	U	A	L
M	R	R	E	E	P	E	C	D	H	I	N	R	C	V	K	S	C
A	M	B	B	T	B	C	E	M	T	C	O	I	S	I	C	R	O
N	E	O	I	M	E	G	A	Y	R	N	L	X	Q	R	A	E	N
A	D	O	U	S	N	L	T	H	G	C	E	A	W	U	B	K	T
G	N	N	S	A	W	H	Y	T	R	E	W	Q	I	S	E	C	R
E	F	A	H	A	E	B	R	U	T	E	F	O	R	C	E	A	O
R	I	C	R	F	A	D	E	D	I	C	A	T	E	D	E	H	L
I	E	E	T	Q	K	E	T	B	E	W	K	R	A	D	V	P	S
E	S	R	O	H	N	A	J	O	R	T	N	O	S	R	E	P	S

Word Search

Auto lock
Backup
Breach
Brute force
Change defaults
Dark web
Dedicated
Deep web

Devices
Email
Encryption
Hackers
Identity theft
Limit access
Malware
Password manager



Numbers
PAO
Parental controls
Pass phrase
Person
PIN code
Qwerty
Special characters

Stay informed
Strong
Trojan horse
Unique
Verification
Virus
VPN
Weak

NOTE: In Acrobat, you can highlight the letters (one by one) as you find them and the words in the list using the highlighter tool on the menu bar.