GABBY'S

CYBER SECURITY AWARENESS

Tips for Friends & Family

CYBERSECURITY AWARENESS MONTH

CYBERSECURITY GUIDEBOOK

Each page has a 'Back to Top' button to quick jump back here.

Table of Contents

INTRODUCTION 2

1. KEEP YOUR APPS AND DEVICES UP TO DATE 3

2. INSTALL ANTI-MALWARE SOFTWARE 3

2. DO NOT OPEN JUST ANY FILE YOU RECEIVE 3

3. PAY ATTENTION TO WHAT YOU YOU'RE ACCEPTING 4

4. USE STRONG PASSWORDS & A PASSWORD MANAGEMENT TOOL 4

5. USE TWO-FACTOR OR MULTI-FACTOR AUTHENTICATION 5

6. CREATE A SECURE EMAIL USED ONLY AS YOUR RECOVERY EMAIL 5

7. PROTECT YOUR INFORMATION 5

8. DO NOT STORE PASSWORDS OR CREDIT CARD INFO 6

9. BE CAUTIOUS WITH PUBLIC WI-FI 6

10. MONITOR YOUR CREDIT 6

SOFTWARE AND TOOLS 7

- Best Password Manager 7
- Free Anti-Malware 7
- Clear Your Privacy Trackers 7
- Best Secure Email 7
- Free Secure VPN 7
- Best Private Search Engine 7
- Free Credit Monitoring and Reports 7

GUIDES AND HOW-TO'S 7

- How to Ensure Ransomware Protection Is Turned On (Windows) 7
- Search for Yourself On A Breach Data Site 7
- How to Remove Your Information from Public Search Engines to Gain Better Privacy 7
- How to Create Secure Answers for Security Questions 7
- Credit Card Safety 7

AFTERWORD 8

OCTOBER IS CYBERSECURITY AWARENESS MONTH

INTRODUCTION

I have recently come to the realization that a lot of my friends and family aren't aware of some of the risks there are online, or don't know what to do to better protect themselves against threats. October is Cybersecurity Awareness Month, and in the spirit of this, I created a little 'guidebook' you can use to help develop better habits in today's digital age. It's important to keep in mind that this list is not exhaustive, and much of the information or suggestions here can change in the near future due to the ever-changing technological industry.

Cybercrime is one of the biggest challenges that humanity will face in the next two decades. Cyberattacks are the fastest growing crime globally, and they are increasing in size, sophistication, and cost. The "Cyber's Most Wanted" list on the FBI website featured 63 notorious people in 2019, up from 19 in 2016[1]. Cybersecurity Ventures, the world's leading researcher for the global cyber economy, expects global cybercrime costs to reach $10.5 trillion annually by 2025, up from $3 trillion in 2015[2]. If it were measured as a country, then cybercrime would be the world's third-largest economy after the U.S. and China.

The sad thing is that these numbers are actually a lot lower than the reality. Cybercrimes are vastly undercounted because they aren't usually reported[3]. The unit chief at the FBI's Internet Crime Complaint Center (IC3) stated that the number of reported cybercrimes in the agency's reports only represent 10 to 12 percent of the total number actually committed in the U.S. each year. And yet, in 2017, the IC3 received nearly 50,000 complaints from victims over the age of 60 with adjusted losses in excess of $342 million — more than all other age groups[4].

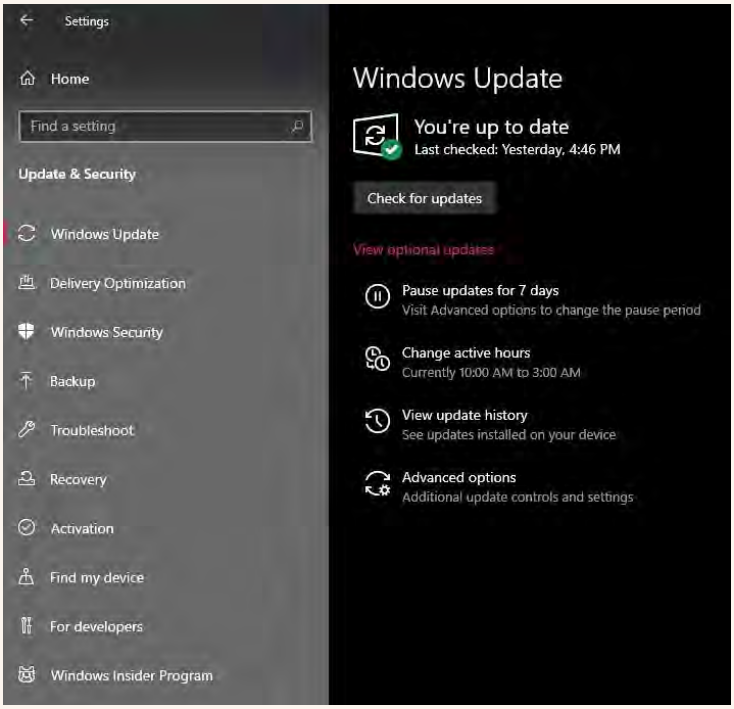
Last year, the Identity Theft Resource Center reported that the newest trends show hackers are accumulating logins and passwords, resulting in a time of rising identity fraud. To make matters worse, funding for support for victims of identity crimes is dropping. Their data show 878 cyberattacks reported in 2020, with 169,575,338 individuals impacted. Out of the 2 types of attacks, phishing victims made up 44% of those affected. **In addition, 36% of 130,043,536 individuals impacted by compromises resulting from human and system errors were attacked through correspondence (e.g., email, letter)[5].**

I firmly believe that the first, and best, course of action is education. This is pretty true in all areas, but especially in the technological department. In addition to the following tips, I have provided infographics with various information ranging from statistics to suggestions. I want to help ***all*** of my friends and family to safeguard their lives, as the vast majority of us transition more and more to digital living.

Without further ado, here are 10 tips I have curated in areas I have found my family and friends struggle with.

[1] https://www.fbi.gov/wanted/cyber
[2] https://cybersecurityventures.cocm/cybercrime-damages-6-trillion-by-2021/
[3] https://slate.com/technology/2018/02/the-real-reasons-why-cybercrimes-are-vastly-underreported.html
[4] https://www.ic3.gov/Media/PDF/AnnualReport/2017_IC3Report.pdf
[5] https://youtu.be/mJird9x8eeo

GABBY'S TIPS



1. KEEP YOUR APPS AND DEVICES UP TO DATE

This is probably one of the easiest habits you can develop to keep your computers, information, and data safe. All devices come with some sort of basic anti-malware software that won't be able to check databases for new virus definitions if it hasn't been updated. Updating also allows them to be 'patched' if a vulnerability is found. Turn on automatic updates so that your device will automatically do it when an update is available. If you need help in figuring out how to enable automatic updates, here is a guide for Android users, here is a guide for Windows, and here is a guide for Apple users.

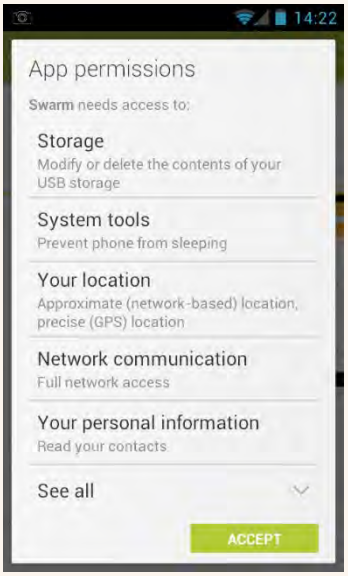
2. INSTALL ANTI-MALWARE SOFTWARE

Anti-malware software has been the most prevalent solution to fight malicious attacks. Antivirus usually deals with the older, more established threats, but anti-malware typically focuses on newer stuff. Anti-malware also typically updates its definitions faster than antivirus, meaning that it's the best protection against new malware you might encounter while surfing the net. Use anti-malware software from trusted vendors and only run one tool on your device. The exception is the default Windows Security. Most software will run alongside Windows' native Virus and Threat Protection. One of the most effective anti-malware apps out there is Malwarebytes. They offer a free version that still stands heads above others, and is available on Windows, iOS, and android.

2. DO NOT OPEN JUST ANY FILE YOU RECEIVE

This includes links via text or email too! Getting you to click on links or open files is called phishing, and it's usually the first step in most malware processes. Hackers become pros at social engineering, which is the art of exploiting human psychology, rather than technical hacking techniques, to exploit vulnerabilities. Attackers will customize phishing attacks to target known interests (e.g., favorite artists, actors, music, politics, news) that can be leveraged to trick you into divulging credentials, clicking a malicious link, or opening an attachment that infects your system with malware. So, say you recently did a bunch of searches for cheap car insurance. Hackers might engineer an attack that looks like an email or text claiming to have a special discount for you, or a bundle package of both auto and life insurance, at a really cheap rate. You click on the link or open the file, and a hidden script within that file activates, creating a backdoor to your system. The hacker can then access your computer at any time, and see exactly what you see. All the log in and credit card info you type in will be visible. They can activate your camera or microphone to take pictures or listen in on your conversations. Or you could become another infected PC connected to a botnet, essentially becoming a threat to others. A general rule of thumb you can abide by is: **Unless you specifically requested a file sent to you, do not open any attachments**. Don't open email from people you don't know. Malicious links can come from friends who have been infected too. So, be extra careful!

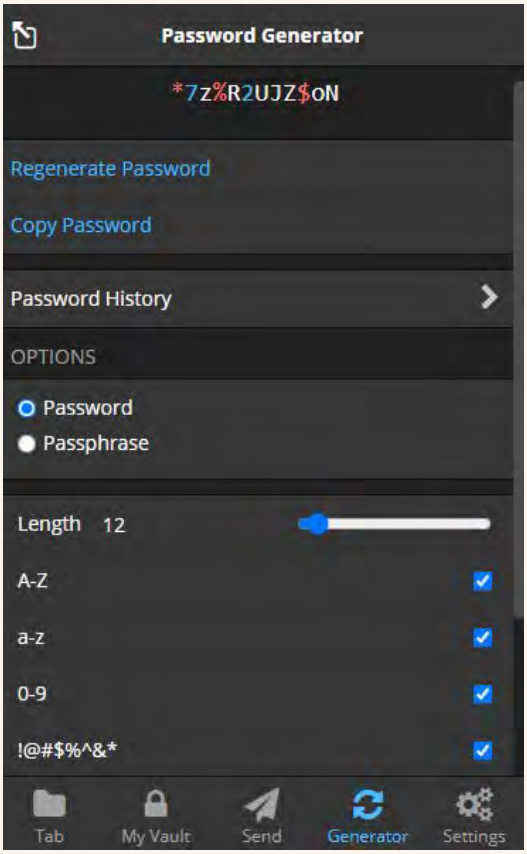
3. PAY ATTENTION TO WHAT YOU YOU'RE ACCEPTING



When you install new software or apps, you will be prompted with questions that allow the program to install itself. The majority of the time, we keep clicking 'next' to speed through the process. What a lot of people don't know, however, is that adware or other programs and settings get tacked on. This means that when you are installing something, you're flying through clicking 'accept' or 'next' for unwanted software that installs on your computer. For mobile users, some apps will ask for permission to access photos and other personal information. Stay informed so you aren't sharing anything you don't want to. Only turn location settings on when you need it, like when using GPS. Here are some examples:

4. USE STRONG PASSWORDS & A PASSWORD MANAGEMENT TOOL

Don't use the same password twice and change it once per year as a general refresh. Include a combination of uppercase letters, lowercase letters, numbers, and special characters to make a password with at least 12 characters. 15 is preferable. Avoid creating passwords with personal information that others may know or would be easy for others to find out (e.g., birthdays, nicknames, anniversaries). Also avoid using words in the dictionary, like "thisisthenewme" or any variation of it, and patterns like "abc" or "123". Passwords using patterns or words commonly found in the dictionary can be 'brute forced' by a hacker. Brute-force attacks take advantage of automation to try many more passwords than a human could, breaking into a system through trial and error. More targeted brute-force attacks use a list of common passwords to speed this up, called dictionary attacks, and using this technique to check for weak passwords is often the first attack a hacker will try against a system. It is also fairly easy to do, even for beginners. **On average, a hacker will brute force crack a 10-character password in 1 week. It will take 1.49m centuries to crack a 15-character password.** Use a password management tool like Bitwarden to keep track of all your passwords. It also has a password generator to create strong passwords for you, and best of all: *it's free*.



Don't store your passwords on sticky notes or in your mobile devices or other files that a hacker can gain access to. If they were able to access your mobile devices file system, you just let them gain access to *all* of your accounts rather than just your phone. An example of a good password generated by Bitwarden is shown to the right. Bitwarden is available on iOS, Windows, and Android. It can also fill in your passwords for each site for you!

Also: when making security questions, **don't answer honestly**. Questions like "What is your mother's maiden name?" can be found on birth certificates or other public documents. Here is a good guide that will help you create secure answers.

5. USE TWO-FACTOR OR MULTI-FACTOR AUTHENTICATION

Two-factor or multi-factor authentication is a service that adds additional layers of security to the standard password method of online identification. Without two-factor authentication (2FA), you would normally enter a username and password. But, with 2FA, you would be prompted to enter one additional authentication method such as a Personal Identification Code, another password or even fingerprint. With multi-factor authentication, you would be prompted to enter more than two additional authentication methods after entering your username and password.

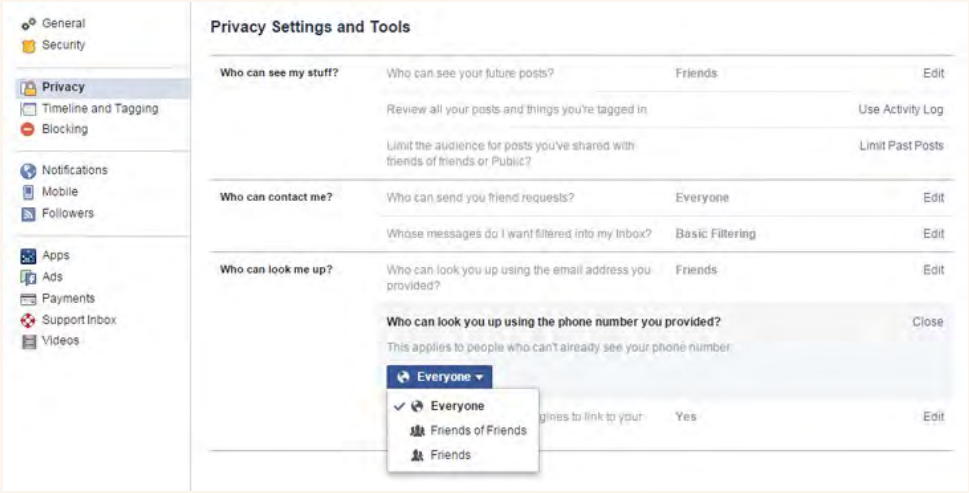
6. CREATE A SECURE EMAIL USED ONLY AS YOUR RECOVERY EMAIL

Your level of digital security is only as strong as the level of your weakest recovery email account's security. Your recovery, or "alternate", email address is an additional email address you list in your security settings to use when you are unable to sign in normally or forget your password. A recovery email address should be on a different and more secure email service, such as ProtonMail. ProtonMail is the world's largest secure email service. They offer end-to-end encryption and store your data in secure data centers located in Switzerland- a country with some of the strictest privacy laws. They ensure your communications are kept private- even they have no way of reading them, so you can rest assured that they can't be read by third parties either. They also offer a free VPN for extra security should you want it.

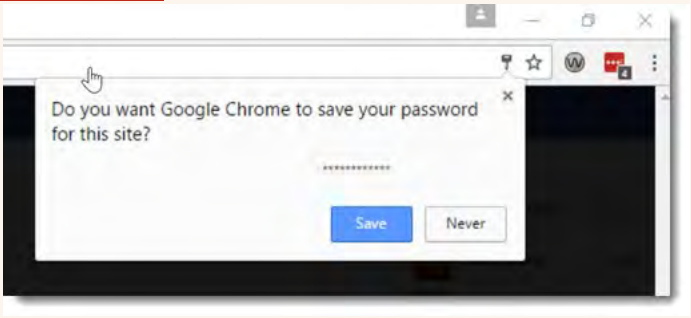
You should also consider using a separate email address, not your private or secure one, to subscribe to email lists. A separate 'junk' email for newsletters, apps, or websites that send frequent emails, coupons, event notifications, sales promotions, or other types of regular communication is a great way to keep your email clutter and spam free. While newsletters are a great way to stay informed about topics you're interested in, the downside is that your inbox may quickly become cluttered. Emails that would be nice to read leisurely get mixed in with important emails, and they may become spammy and inhibit your ability to see your sensitive emails. It is not recommended to use this account for any other activities or to use this email address for shopping on a website. **Remember, the more websites that have your email on file, the more chances there are for your sensitive data to be exposed.**

7. PROTECT YOUR INFORMATION

Personal Identifiable Information (PII) is any information that can be used by a cybercriminal to identify or locate an individual. In the "always-on" world of social media, you should be very cautious about the information you include online. **Adding your home address, birthdate, or any other PII information will dramatically increase your risk of a security breach.** Hackers use this information to their advantage!

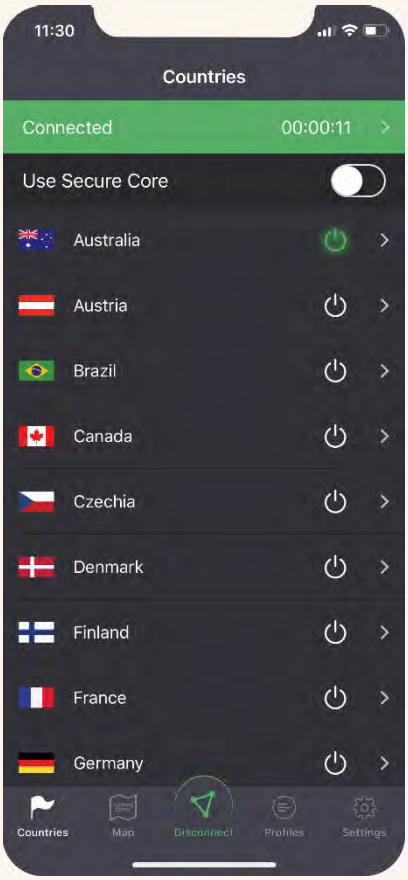


8. DO NOT STORE PASSWORDS OR CREDIT CARD INFO



Storing passwords, usernames, or credit card numbers on your computer seems like the perfect solution to the conundrum of trying to remember all the information, especially when following experts' advice to not repeat passwords. **But browsers save passwords in a list you can pull up to view anytime, which a lot of viruses and malware can steal remotely**. This article shows how hackers can extract your passwords using only 12 lines of code. A password manager like Bitwarden is an encrypted data vault that locks automatically when not in use, so hackers would have to try to breach it to access your passwords.

Even if you don't save your passwords to your browser, you can still be at risk if you store credit card numbers when shopping online. Storing credit card info to expedite checkouts on websites such as Amazon or Walmart.com may seem logical if you use them frequently, but if that website were to ever have a data breach, your credit card number may be exposed. Experian has an article with tips to keep you safe. Bitwarden also has the option to store credit card numbers if you truly want to save your information for ease of access.



9. BE CAUTIOUS WITH PUBLIC WI-FI

Unsecured networks can be used by anyone to propagate malware and access sensitive information. One of the most dangerous aspects of free Wi-Fi is the ability of hackers to place themselves between you and the connection point. So, rather than communicating directly with the hotspot, you wind up transmitting your information to the hacker. They will also have access to all of the info4rmation you send out, including emails, phone numbers, credit card information, and so on.

The simplest solution is to not use public Wi-Fi at all, but if you have to, the best method you can use to protect yourself is to use a Virtual Private Network (VPN). By using VPN software, the traffic between your device and the VPN server is encrypted. This means it's much more difficult for a cybercriminal to obtain access to your data on your device. Use your cell network if you don't have one, but ProtonMail offers a free VPN when you sign up for the world's most secure (*and free!*) email.

10. MONITOR YOUR CREDIT

With the surge in cyberattacks, it's more crucial than ever for people to protect their accounts and keep an eye on their credit reports. Right now, the most efficient strategy to safeguard your personal credit information from hackers is to implement a credit freeze. It essentially allows you to lock your credit and utilize a personal identification number (PIN) known only to you. You can then use this PIN when applying for credit.

credit karma

If a credit freeze is not something you can or are willing to do, you can still take steps to safeguard your identity. There are several websites that offer a free credit report. The only official government-supported website is annualcreditreport.com, but you can only view it for free once yearly from each of the credit bureaus. While this is still highly encouraged, you can also sign up for websites like creditkarma.com to access your information any time you want. They also send you credit alerts if anything important changes on your TransUnion credit report. This can help you spot identity theft and fraud. They also offer financial calculators and educational articles if you're interested.

RESOURCES

SOFTWARE AND TOOLS

Best Password Manager
https://bitwarden.com/

Free Anti-Malware
https://www.malwarebytes.com/

Clear Your Privacy Trackers
https://www.ccleaner.com/

Best Secure Email
https://protonmail.com/

Free Secure VPN
https://protonvpn.com/

Best Private Search Engine
https://duckduckgo.com/

Free Credit Monitoring and Reports
https://www.creditkarma.com/

https://www.annualcreditreport.com/

GUIDES AND HOW-TO'S

How to Ensure Ransomware Protection Is Turned On (Windows)
https://bit.ly/3uTGvNG

Search for Yourself On A Breach Data Site
https://haveibeenpwned.com/

How to Remove Your Information from Public Search Engines to Gain Better Privacy
https://the.osint.ninja/optoutdoc

How to Create Secure Answers for Security Questions
https://bit.ly/3iJSSXM

Credit Card Safety
https://bit.ly/3ajAgcv

AFTERWORD

Like I said in the introduction, this list is most definitely not exhaustive. Cybersecurity is a whole field of study (trust me, I know!) and to truly understand the implications would take a lot more that 7 pages. These are just the things I have observed as potential issues among my family and friends. Also keep in mind that *there will always be a way around these*. They are not 100% guaranteed to prevent all attacks. But having a basic understanding of what better habits look like will decrease the chances **dramatically**.

Now, I'm not an expert (yet!), but as many of you know, before enrolling at OCCC, cybersecurity was a **hobby** of mine. More specifically, 'ethical hacking'. I studied constantly, venturing onto the deep web to find free educational material that would otherwise cost tons of money. I took online classes such as Introduction to Computer Science Using Python from MIT or Learn Ethical Hacking from Scratch that teaches using methods and mindsets just like black hat hackers. I couldn't afford the cost of getting credit for these classes, but I gained the knowledge, nonetheless. And let me tell you- it's all too easy. **Too easy**. Let me give you a personal example that I probably shouldn't.

I found an article on one of the blogs I follow that showed you how to make a Wi-Fi attack platform using a Raspberry Pi- a minicomputer the size of a credit card. They are capable of cracking wireless networks, jamming Wi-Fi for blocks, tracking cell phones, listening in on police scanners, and can apparently even shoot a missile into a helicopter. *All for the low cost of $35*. For less than a tank of gas, a Raspberry Pi 3 buys you a low-cost, flexible cyberweapon. But imagine if you could turn this device, which was created to teach children computer science, into a persistent backdoor or ransomware attack in only 30 seconds. The article I found combined it with a Rubber Ducky, which can be plugged into nearly any computer to control it as a keyboard. You can craft new payloads that could remotely execute commands on a subject's computer. It automates complex tasks into a single payload- without the average computer ever detecting it.

I experimented with the capabilities of it, using it on my home network to see if I could try to figure out how to read data packets. I was able to view the packets, but I didn't know how to make sense of it. However, I noticed more information than I should have. It turns out, I captured my neighbors' data as well. A hacker, even if unintentionally, could have gathered who knows how much information on them. I couldn't read it, but I *did* understand one thing: their network security was extremely low. There were 3 immediate residences with the untranslated data, and if I had kept the program running, it would have sniffed more.

The moral of the story is: be safe. Be smart. People share so much data on social media alone- where they are, who they are with, their likes, their hobbies. Even the US Government shares so much information. Hackers used to have to "dumpster dive" to get info; now, our sensitive data is mostly online. And it's available for "others" to retrieve. Protect your data, protect yourself. Make it a conscious effort every day and it becomes second nature. I know the suggestions I listed sound like a lot, but I use every single one of them every day and I barely have to think about it. **Make your privacy a priority.**

The remaining pages are infographics that I created, or (in the case of the last 3) I found. There is a wealth of knowledge out there if you want to take it even further. I learned everything I know, as of today, for free online. I love you all and I am only an email away if you have any questions.

Best of luck!

CYBERSECURITY AWARENESS MONTH

CYBERSECURITY

Back to Top

TIME IT TAKES A HACKER TO BRUTE FORCE YOUR PASSWORD

National Cyber Security Awareness Month

Number of Characters	Numbers Only	Lowercase Letters	Upper and Lowercase Letters	Numbers, Upper, and Lowercase Letters	Numbers, Upper, and Lowercase Letters, Symbols
4	Instantly	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	Instantly	Instantly	Instantly
6	Instantly	Instantly	Instantly	1 sec	5 secs
7	Instantly	Instantly	25 secs	1 min	6 mins
8	Instantly	5 secs	22 mins	1 hour	8 hours
9	Instantly	2 mins	19 hours	3 days	3 weeks
10	Instantly	58 mins	1 month	7 months	5 years
11	2 secs	1 day	5 years	41 years	400 years
12	25 secs	3 weeks	300 years	2k years	34k years
13	4 mins	1 year	16k years	100k years	2m years
14	41 mins	51 years	800k years	9m years	200m years
15	6 hours	1k years	43m years	600m years	15bn years
16	2 days	34k years	2bn years	37bn years	1tn years
17	4 weeks	800k years	100bn years	2tn years	93tn years
18	9 months	23m years	6tn years	100tn years	7qd years

Made by Gabrielle Decker | Data Sourced from HowSecureismyPassword.net

Gabby's Checklist

- [x] Up to date
- [x] Using anti-malware
- [ ] Clicking files
- [x] Installation Caution
- [x] Strong Passwords
- [x] 2FA
- [x] Secure Email
- [x] Info Protection
- [ ] Credit card storing
- [x] Monitoring Credit

List made by Gabrielle Decker

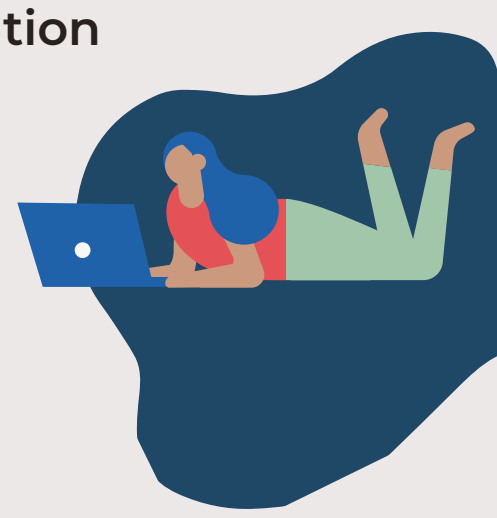
7 INTERNET SAFETY TIPS

FOR EVERYONE!

1

Don't Give Out Personal Information

Avoid online phishing attempts by keeping your personal information private. Don't give out your phone number, social security information, or banking info to someone you don't know.



2

Create Complex Passwords

Create passwords with a combination of letters, numbers, and symbols. Consider using password managers to create and keep track of your passwords.

3

Check Website Reliability

Before purchasing anything on a website ensure that it's safe. You can do this by checking if it has a small lock icon or "https" before the URL. The "s" in "https" stands for "secure" and the lock means it's confirmed as a safe site by your browser.

4

Avoid Suspicious Online Links

Be careful of websites or emails containing suspicious links. Some websites may use quizzes, freebies, or salacious stories to get you to click on them and then steal your personal information.

5

Keep Your Computer Updated

Computer developers release updates to keep products safe. Keep your device software up to date so it is not vulnerable to malware.

6

Monitor App Permissions

Learn the privacy settings for any device, app or service you use. Some apps will ask for permission to access photos and other personal information. Stay informed so you aren't sharing anything you don't want to.

7

Be Cautious with Public Wifi

Be careful when you use public wifi. When accessing public networks, anyone can use unsecured networks to distribute malware and access private information.

Online safety guidelines

STRONG PASSWORDS

Quick tips for creating and saving your online passwords

ADD VARIETY

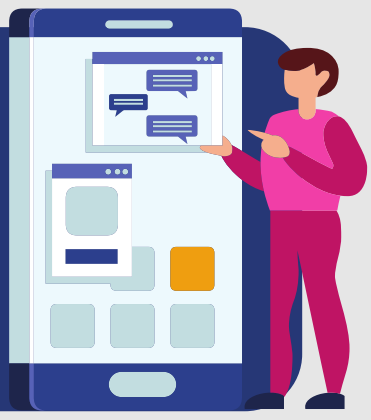
Use uppercase, lowercase, numbers, & special characters. Avoid any words in the dictionary, like “thisisthenewme”, and patterns like “abc” or “123”

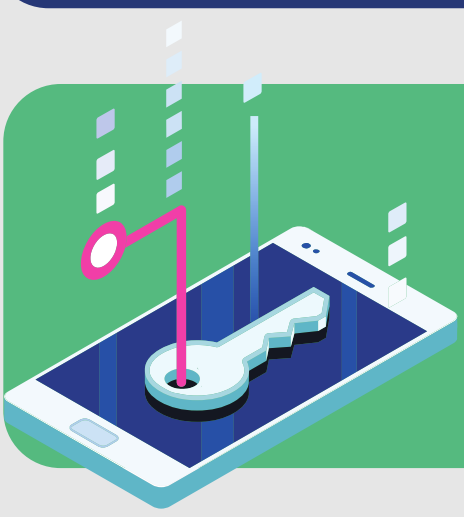
DON'T RECYCLE

Don't use the same password for all of your accounts. Even better, try not to use the same password twice.

AVOID PERSONAL INFO

Don't use personal information that others may know or would be easy for others to find out like birthdays, nicknames, or anniversaries.





MAKE IT LONG

Use passwords with at least 12 characters, 15 when possible.

CHANGE OFTEN

Make sure to review your passwords and change them at least once a year. Every 6 months is better.

USE A MANAGER

Password management apps can help keep track. Some, like Bitwarden, will generate passwords for you (and it's free).

Did You Know?

In 2014, nearly half of Americans had their personal info exposed by hackers – and that doesn’t even count the many companies that experienced breaches[1].

Sources

[1] https://www.betterbuys.com/estimating-password-cracking-times/

CYBERATTACKS

CAN OCCUR MANY WAYS, INCLUDING[1]:

01.

Accessing your personal computers, mobile phones, gaming systems and other internet and Bluetooth connected devices

02.

Damaging your financial security, including identity theft

03.

Blocking your access or deleting your personal information and accounts.

04.

Targeting children & the elderly

05.

Complicating your employment, business services, transportation and power grid.

sources

[1] Ready, an official website of the United States Government
https://www.ready.gov/cybersecurity

[2] 2019 Cybersecurity almanac
https://cybersecurityventures.com/cybersecurity-almanac-2019/

TIPS FOR CONNECTING TO PUBLIC WI-FI

01 DON'T TOUCH ANY PERSONAL INFO

Avoid using any Personally Identifiable Information (PII), including banking info, social security numbers & home addresses at all costs. Some accounts require things like phone numbers to sign up, so you may not remember entering it, inadvertently allowing access to personal information.

USE A VIRTUAL PRIVATE NETWORK 02

A VPN allows you to create a secure connection to another network over the Internet. VPNs can be used to access region-restricted websites, shield your browsing activity from prying eyes, and more.

03 USE SSL CONNECTIONS

When browsing the internet, be sure to enable the "Always Use HTTPS" option on websites that you visit frequently, including any and all sites that require you to enter any type of credentials. SSL adds a layer of encryption to your connection.

INVEST IN AN UNLIMITED DATA PLAN 04

This will not only eliminate your need for accessing insecure Wi-Fi networks, it will also often allow you to use your mobile device to create a personal internet “hotspot,” meaning a VPN connection wouldn’t even be necessary.

05 TURN OFF SHARING

You don't really need file sharing when connecting to McDonalds Wi-Fi, or on the road to the airport. Turn it off in system preferences or control panel for phones. For PCs, Windows can do it for you by choosing the "public" option the first time you connect to a new, unsecured network

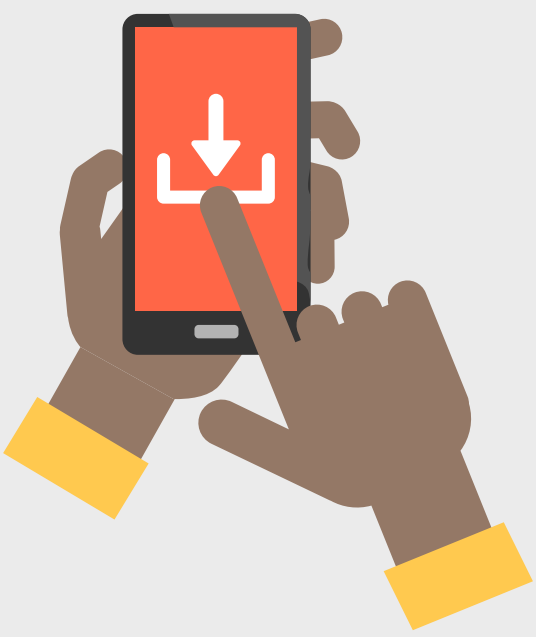
National Cyber Security Awareness Month

Microsoft

Tech support scams and how to avoid them

If you haven't experienced a tech support scam yet, chances are you know someone who has. As part of **National Cyber Security Awareness Month,** Microsoft has released the results of a new global survey. Findings from the survey include:

2 out of 3 people have experienced a tech support scam in the last 12 months.



1 in 5 consumers surveyed continued with a potential fraudulent interaction, which could mean they downloaded software, visited a scam website, gave the fraudsters remote access to their device, or provided credit card information or other form of payment.

Nearly 1 in 10 have lost money to a tech support scam.

Of those who continued with a fraudulent interaction, **17% of them were older than 55, while 34% were between the ages of 36 and 54.**

50% of those who continued were millennials, between the ages of 18 and 34.

If someone claiming to be from a reputable software company, calls you:

- Do not purchase any software or services.
- Never give control of your computer to a third party unless you can confirm that it is a legitimate representative of a computer support team with whom you are already a customer.
- Ask if there is a fee or subscription associated with the "service." If there is, hang up.
- Take the person's information down and immediately report it to your local authorities.

STOP | THINK | CONNECT®

Microsoft

CYBERSECURITY AWARENESS MONTH

NATIONAL CYBERSECURITY ALLIANCE

YOUR CONNECTED HEALTHCARE

The convergence of the internet and healthcare has created many benefits for patients and healthcare providers, but has also created vulnerabilities that cyber criminals regularly attempt to exploit. This infographic shares some of the most common ways patients and medical practitioners access health data using technology, and highlights tips to help you Do Your Part. #BeCyberSmart

TELEHEALTH

Telehealth is the use of technologies, such as computers and mobile devices, to access health care services remotely if patients and healthcare providers can't be in the same place at the same time.

TIP #1

Be sure your software is updated on your devices before engaging in a telehealth session and connect via a secure wifi connection to protect your session.

WEARABLE HEALTH TECHNOLOGIES

Consumers are increasingly using wearable technologies (such as smart watches and heart rate monitors) for continuous monitoring of their health and wellness activities.

TIP #2

Before purchasing a wearable technology, research the manufacturer & review the company's privacy policy to determine what steps they take to protect your data.

HEALTH & WELLNESS APPS

Whether you're wanting to manage your diabetes, get medication reminders, or track your exercise routine, there's an app for that! Apps are a great way to actively manage your health and wellness efforts.

TIP #3

Review the details of any health app before downloading. Only download from trusted sources, and read reviews prior to downloading. Immediately configure your privacy and security settings to limit how much information you share.

ELECTRONIC HEALTH RECORDS

Electronic Health Records are a digital version of a patient's paper chart, making information available instantly and securely to authorized users.

TIP #4

Make a long, unique passphrase to access healthcare accounts. Length trumps complexity. A strong passphrase is a sentence that is at least 12-15 characters long.

STAYSAFEONLINE.ORG
@STAYSAFEONLINE
/STAYSAFEONLINE

HOW TO CREATE THE PERFECT PASSWORD

16 MINUTES
The time it took Jeremi Gosney, CEO of Stricture Consulting Group, to crack 16,223 passwords.

facebook 600,000
The number of hackers that log into Facebook every day trying to breach users' personal security.

$1 BILLION
The amount hackers take from small to medium sized banks in Europe and the U.S. every year.

Don't let your accounts be easy targets.
Read below to learn how to produce the perfect password.

WEAK	MEDIUM	STRONG
abc — Made up of lower case characters only	a2c — Mix of characters & numbers	bY!4 — Combination of upper & lower case letters, numbers & symbols
Use your name, your pet's name, your birthday, other common names	1-8 — At least 8 characters long	8+ — 8+ characters long
1-6 — 1 – 6 characters long	Abc — Both lowercase & uppercase	Aa1* — Upper & lowercase, numbers, symbols
Incorporate dictionary words	6&! — Include a number or symbol	B!g d0G5 — Contain made-up phrases
Repeat previously used passwords	No dictionary words	No complete words
QWE RTY — Contain keyboard patterns or swipes		W4f!dt W6Tb*7& — Changed regularly to prevent hacking / exposure

HOW TO CREATE THE PERFECT PASSWORD

1 Use lower and upper case letters, numbers and keyboard characters.

2 YRS

George Shaffer, a password expert, says that a **password of eight characters** in length, and one which utilises numbers, letters and keyboard characters, **won't be cracked for two years.**

2 Go for length over complexity.

On average a hacker will 'bruteforce' crack a **10 CHARACTER PASSWORD** in **1 WEEK**

Whilst a **15 CHARACTER PASSWORD** will take **1.49m CENTURIES**

3 Don't use.....

Dictionary words · Slang · Names · Email addresses

Use a passphrase, for example
Dkjf9+fldmsrbly
translates to
Derek jumped for glory and failed miserably

Passphrases are much **easier to remember** than non-sensical words. b4x87g-m?!

4 Get yourself a password manager...

...such as LastPass, KeePass or 1Password.

A password manager will remember all of your passwords, so you don't have to.

Password databases are a highly targeted area for security breaches. None of the major password managers have suffered any breaches, except for LastPass which was possibly breached in 2011 and as a result, have incorporated many new layers of security.

LastPass and 1Password also offer password security for your mobile phone, so **consider a password for your mobile too.**

5 Don't disclose your password details to anybody.

And **don't write your password down** on a Post-It note for all to see. Record it and leave it hidden-away at home.

Think about it this way: you wouldn't leave your front door unlocked if you went on holiday, so why choose to stick your password to your monitor at work?

6 Be vigilant.

Wherever you are watch out for people looking at your laptop screen over your shoulder. **Don't leave your laptop alone for any period of time.**

Even if you are using a free Wi-Fi connection, that doesn't stop somebody in a nearby building looking to steal your data on the same network. So, it's crucial you create the perfect password.

BEST PASSWORD MANAGERS

1Password
$40 (£24)

Benefits
- Multiple vault capacity
- Separate profiles for private & work
- Password audit which detects passwords that haven't been altered for a while

LastPass **
$FREE

Benefits
- Super-strong encryption (even LastPass can't read it)
- More authentication than any other password manager

KeePass
$FREE

Benefits
- Available for all platforms – mobile and desktop
- Includes a random password generator
- Protects against 'keylogging' (when an application or dongle is connected to your computer which logs every keystroke you type; the information then being sent on to a hacker).

Follow these steps and you can be safe in the knowledge that your new password is secure

.....for now.

SOURCES

Creating Strong Passwords - microsoft.com
Tips for creating the perfect password - abc15.com
Password Strength - azteenchallenge.org
Webscape: Perfect passwords - bbc.co.uk
What is Internet Security? - bbc.co.uk
Hackers Take $1 Million a Year as Banks Blame Their Clients - bloomberg.com
Anatomy of a hack - arstechnica.com
Passphrases: A viable alternative to passwords? - darkreading.com
How to Create and Remember Strong Passwords - forbes.com
Passwords - getsafeonline.org
Why Post-It notes are not a safe way to store passwords - insidetechnology360.com
Do I really need to worry about security when I'm using public Wi-Fi? - lifehacker.com
1 Password 4 for Mac review: State-of-the-art password management for everyone - macworld.com
How Strong is your Password? - media.navigatored.com
5 Tips for top-tip Password Security - microsoft.com
How to Create Strong Passwords and Passphrases - movements.org
KeePass Review - pcadvisor.co.uk
LastPass 3.0 - pcmag.com
Password managers: Are they Safe? Which is the Best? - pcpro.co.uk
Password managers: Are they Safe? Which is the Best? (Page 4) - pcpro.co.uk
Password Complexity Policy - portalguard.com
The Simplest Security: A Guide to Better Password Practices - symantec.com
How to Write the Perfect Password - technewsdaily.com
Hackers go after Facebook sites 600,000 times every day - telegraph.co.uk
Tips for Creating a Strong Password - windows.microsoft.com

Presented by
WhoIsHostingThis?