Cybersecurity Awareness Month
31 Tips for Staying Safe

1

Cyberbullying Safety Tips for Parents

Cyberbullies are taking advantage of technology to harass our loved ones.
As parents and mentors we can take steps to protect them.

- Teach our loved ones good online habits.
- Always keep communication open.
- Look for the warning signs.
- Document the activity if it is brought to your attention.
- Report it to the proper authorities.

2

Minimize the Access Others Have to Your Information

Easy habits to adopt like creating strong passwords, using a password manager, enabling multi-factor authentication when available, and using security questions properly may dramatically reduce the chances, when used consistently that the information on your computer will be lost or corrupted.

3

Use USB drives Safely

USB and portable hard drives are popular ways for storing and transporting data, the same things that make them convenient also introduce security risks. Take advantage of security features like adding encryption to your USB drives to protect your data. Disable the Autorun feature. It can cause unwanted or harmful media to automatically open.

4

Do's and Don'ts of password creation

When coming up with a strong, easy to remember password it is tempting to reuse it – don't!
Do: use the longest password or passphrase permissible by each account, consider developing mnemonics to remember to remember complex passwords, use a password manager
Don't: Do not use passwords based on personal information, do not reuse passwords, do not share your password with anyone

5

Protect Personal Information

Always make sure to verify who you are sending personal information to and if you are submitting personal information to a website verify that they have a privacy policy in place.
To protect your identity and prevent attackers from easily accessing information about you, be cautious providing your date of birth, social security number, or other personal information online.

6

Holiday Travel with Personal Internet-Enabled Devices

With holidays right around the corner, you are probably getting ready to take a fun and relaxing vacation.
With the internet at our fingertips, you need to know how to protect yourself from risks.

- Don't connect to public WiFi, use your cellular data or a personal hotspot
- Turn Bluetooth off when not in use.
- Be cautious when using charging stations
- Remember to be cyber safe this holiday season!

7

Use Caution with Email attachments

Just because an email looks like it came from someone you know and trust that doesn't mean it did, so be wary of unsolicited attachments, even from people you know.
If an email or attachment seems suspicious, don't let your curiosity put your computer at risk.

8

Tips to avoid social engineering attacks

Social engineering attackers use human interaction to gain or compromise information about an organization or its computer systems.
Being aware that scammers can pose as friends, family or new employees will give you the confidence to be suspicious.
Not everything sent to you online is a scam, remember to do your due diligence and verify the who is asking for your personal information.

9

Transferring Cryptocurrency Safely

Cryptocurrency addresses are long and complex, when you are sending crypto to a friend or business you need to make sure the address is correct!
We recommend that you use the QR functionality that most crypto exchanges offer, if a QR code is not available, you can also use the copy and paste function as well.
It is your responsibility as the sender to double and triple check that the person you are sending crypto to is the correct person.
Since the transfer rates are so low, we recommend sending a small amount and verify it sent before sending the full amount.

10

Social Media Safety Tips

- Remember to limit the personal information you post online
- The internet is a public resource, only post things that you are comfortable with others seeing.
- Be wary of strangers friending you online
- Take advantage of social media sites privacy settings
- Talk with your children about being safe online

11

Proper Disposal of Electronic Devices

It is important to follow the best practices for personal device disposal. Laptops, tablets, and smartphones allow you to keep great deals of information. If they are not properly destroyed or sanitized your personal data could fall into the hands of cybercriminals.

12

Home Wi-Fi Security

Many users share two common misconceptions about the security of their home Wi-Fi networks. Their network is too small to be targeted in a cyberattack or their devices are "secure" out of the box. Remember to remain vigilant and understand the risks of being connected to the internet.

13

What is Cybersecurity?

Cybersecurity is a form of art. It helps protect networks, devices, and data from unauthorized access or criminal use. Today, everything relies on smart devices and the internet now.

14

Avoid Useless Downloads

3rd-party downloads are some of the most popular tricks used by hackers to gain access to your data. One safety measure for downloading safely is to choose the process of custom installation, making sure to read each page and declining anything that specifically for the application you are downloading.

15

Think Before you Click

Links in mails in the form of docusign, password recovery emails, and bank statements are some of the most popular methods used by hackers to trick you and gain your personal data.
These fake sites connected to the links are often too similar to the real one.
Hackers will get you to provide your personal details and gain access to your account using the same.
Always verify the URL before clicking on a link, you won't regret it.

16

Review Online Accounts and Credit Reports Regularly

It is easy to become absentminded about changes with our digital lives. Set reminders monthly to check bank accounts, credit reports, or other online accounts for unfamiliar changes.

17

Never Believe You're Secure Enough

Digitally, there is no thing as secure enough.
Cybercriminals find new inventive ways to creep and hack their way into your piece of that world.
You are the best security measure you have.

18

Remember the SLAM Method

Sender- make sure the sender's address is accurate
Links- hover over all links to see where they might take you
Attachments- be cautious and don't open unexpected attachments
Message- if a message feels too urgent, threatening, or suspicious contact IT

19

Plan for the Unexpected

We understand that life gets in the way. Sometimes you may face an unexpected dilemma like your personal data being stolen. You need to have a disaster recovery plan in place, both at work and at home.

20

Anti-Virus & Anti-Malware Aren't a Thing of the Past

While humans are the best (means or weapon) to combat cybercriminals, having a robust anti-virus/malware software is a must. While they are the some of the oldest security protections around, they still work! These programs significantly reduce your vulnerability to an attack.

21

Your IoT devices are at risk too!

Any device connected to the internet is vulnerable to attack.
Yes, that means your fridge!

22

Always Be On Guard

There are no days off with good cybersecurity practices.
Trust your gut. If something looks suspicious, it probably is!

23

Use Strong Authentication Tools

Strong authentication begins by using unique, complex passphrases for all accounts and devices. Pins should be unique to individual devises. Biometric authentication like fingerprints or facial ID are examples of additional authentication.

24

Use Privacy Controls on Personal on Business Social Media Accounts

This keeps personal identifiable information out of public view
Specifically, location, full name, contact information, and close family or friend contacts. Cybercriminals can and will use this information to increase efficacy of attacks.

25

Use an Encryption Service to SecureYour Data

Using an encryption service will allow you to have piece of mind if your personal or work devices are stolen or lost. The encryption won't allow cybercriminals to read it without a specific encryption key. If you need help setting up encryption for your devices, let us know, we are happy to help!

26

Monitor Your Dark Web Presence

Most people don't even want to think about what's happening on the dark web, but it's important to know if your data has been compromised by malicious actors.

27

Backup Data Often and Use Remote Security Features

Remote lock and wipe options can protect personal and business data. Many devices provide encryption tools. Make sure to set up and enable incase of an emergency.

28

Do Not Use Public Wi-Fi

If this is the only option, use a VPN (virtual private network) protect your device from snooping criminals searching for vulnerable target. Do not click on pop up ads if connected public network. These are often used by cybercriminals to deliver malware.

29

Keep your devices safe by staying up to date on OS and security feature updates.

Keeping your operating system, security software, and web browser updated will minimize threats to your network.

30

Educate Your Children or Youth on Cybersecurity Threats toBe Aware of.

It's never too early to start educating youth on cybersecurity. There are three big scam methods to watch for; email, text, and phones calls. A 'too good to be true' concept is often used on unsuspecting users. Teaching this early can help create a strong defense for cybercriminals.

31

Cybercriminals attack any and everyone.

Educating older relatives is just as important as educating the youth and everyone in between. Various scam methods are used to attack those who have trouble grasping new technology. Keeping it simple will help ease into technology for beginners.Teach unsuspecting users the big three methods of attack (email, text, phone). Users should be weary of clicking links and messages and should use a family code word to verify abnormal requests.