**Cybersecurity Hygiene, Best Practices and Tips**

With the move to remote/hybrid work, here are some tips that should be followed.

1. **Only join trusted networks.** Malicious actors can make a network connection that may look legitimate but is actually a fake one used to track your network activity and gather information.
2. **Always lock your laptop when you are not working on it**.
3. **Change default passwords on your home Wi-Fi** **routers**. Internet Service Providers give you a generic password on your router that should be changed once set up.
   1. Only give out this password to trusted individuals.
4. **Utilize Internet Service Provider applications** to monitor the traffic going through your network.
   1. Use this to verify the devices on your network.
5. **Utilize Multi-Factor Authentication on your devices** so that you need more than just a password to access your accounts.
6. **Make sure your home wireless is secured with WPA2.** This is the most up to date, secure wireless encryption protocol.

***Device Best Practices***

Both Organization-owned devices and personal devices must be kept up to date with the latest security to prevent vulnerabilities from being exploited.

1. **Restart your computer at least once a week** to apply the latest Windows Security updates.
2. **Patch your wireless devices** by staying up to date on the operating system updates.
3. **Do not leave your computer unattended in public places**. This could result in theft or unauthorized viewing of information.
4. **Monitor the aging of your computer**. Many devices have a shelf life and if used for too long, they could slow down or have vulnerabilities.
5. **Do not download software from unverified third parties**. These could bring viruses into your network.

***Password Hygiene***

Preventing unauthorized access is essential to protecting the confidentiality of data within the Organization. This helps to protect personal, donor, and company data.

1. **Utilize complex passwords**. These should use lowercase and uppercase letters, symbols, numbers, and phrases. Try not to use single words that can be guessed via a dictionary.
2. **Make use of a password manager service** like LastPass, 1Password, etc.
3. **Do not share passwords**. If you need passwords across the organization (ex. social media) utilize the shared password feature on LastPass or your password manager.
4. **Do not reuse old passwords**. A password breach could occur from years ago, and if you use one of those old passwords, you could still be vulnerable.
5. **Check to see if your email is on the dark web**. You can use [haveibeenpwned.com](https://haveibeenpwned.com/) to find common breaches.

***Watching out for Attacks***

Since remote work has become a staple across society, there are, in turn, more cyber risks and attacks organizations face on a day-to-day basis. As the end user, you must be always aware and follow safe practices to avoid cyber-attacks.

*Phishing*

1. **Be aware of links and attachments**, especially if you were not expecting the email.
2. **If you are unsure about an email, verify separately** with that person to make sure that it came from them.
3. **If there is an urgent message, leading you to a link, be wary** that it might be a phishing attempt.
4. **Always look at the from line and the reply to** make sure you know the email address.

*Social Engineering*

1. **Only accept requests from people that you know on social media**.
2. **If someone is asking for personal information, question why they are doing it**. Do you know them? Could they use this information to crack a password?
3. **Help desks should not ask for your password**. If they do, they could be acting maliciously. If you do share your password, change it immediately.

*Malware*

1. **Do not download random software** as this could bring in a virus, worm, or Trojan horse.
2. **If you do click on a virus, notify management immediately and disconnect from the network.**

***Following Organizational Best Practices***

The Organization has set up your devices to be secure and provide support when there are any questions relating to security. There are policies and procedures set up to protect you from cyber-attacks.

1. **Do not uninstall anti-virus or anti-spyware**. The Organization has installed antivirus, antimalware and endpoint protection which is used to protect your computer from the attacks above.
2. **Work equipment is owned by the Organization and there should be no expectation of privacy**. Anything stored on the device will be treated as business related.
3. **Unverified or unapproved software should not be installed on Organization machines**.
4. **Gaining unauthorized access to files or folders is not allowed**. If you access or have access to something that is not related to your job function, let management know so it can be updated.
5. **The Information Security Policy should be always followed**. Lack of following can result in unintended risks for the Organization and each person in the organization.