BE ALERT

TOP 10 CYBER TIPS

1:

PRACTICE GOOD PASSWORD MANAGEMENT.

Use a strong mix of characters or a paraphrase like "Cupst@rHOr$e", and don't use the same password for multiple sites.

Its best not to share your password with others, and definitely don't write it down where it can be found. Using a password manager app is an excellent way to store passwords and keep them safe.

2:

NEVER LEAVE YOUR DEVICES UNATTENDED.

If you need to leave your computer, phone, or tablet for any length of time, no matter how short, lock it up so no one can use it while you're gone. If you keep sensitive information on a flash drive or external hard drive, make sure to lock it up as well.

3:

SENSITIVE BROWSING, SUCH AS BANKING OR SHOPPING, SHOULD ONLY BE DONE ON A DEVICE THAT BELONGS TO YOU, AND ON A NETWORK THAT YOU TRUST.

Whether it's a friend's phone, a public computer, or a cafe's free Wi-Fi, your data could be copied or stolen.

4:

MAKE SURE YOU HAVE ANTI-VIRUS OR ANTI-MALWARE SOFTWARE, AND THAT IT IS ALWAYS UP TO DATE.

Having a current and up to date product will protect you against the current threats. Most vendors make automatic updates available. There are many free and paid products that are reputable, look up reviews on https://forums.whirlpool.net.au

5:

ALWAYS BE CAREFUL WHEN CLICKING ON ATTACHMENTS OR LINKS IN EMAIL, THEY COULD BE PHISHING MESSAGES!

If it's unexpected or suspicious for any reason, don't click on it. When you receive an email, consider who is emailing you and what they are asking you to do. If you are suspicious about the email, call the business or person using contact details obtained from a website or other legitimate source. Be wary of emails with links asking you to change passwords, they are phishing attempts.

NSW GOVERNMENT | TAFE NSW

BE ALERT

TOP 10 CYBER TIPS

6:

THINK ABOUT WHAT YOU PLUG IN TO YOUR COMPUTER, AND BACKUP YOUR DATA REGULARLY.

Malware can be spread through infected flash drives, external hard drives, free Wi-Fi networks and even smartphones. A recent backup is the best way to recover lost data, so make a backup today.

7:

WATCH WHAT YOU'RE SHARING ON SOCIAL NETWORKS. CHOOSE WHO YOU SHARE YOUR PERSONAL INFORMATION WITH, AS WE ALL SHARE FAR TOO MUCH TO LARGER AUDIENCES.

On Facebook and similar sharing apps, criminals can befriend you and easily gain access to a shocking amount of information, where you go to school, where you work, when you're on vacation, that could help them gain access to more valuable data. Make identity theft from social media harder by reviewing your privacy and security settings.

8:

OFFLINE, BE WARY OF SOCIAL ENGINEERING, WHERE SOMEONE ATTEMPTS TO GAIN INFORMATION FROM YOU THROUGH MANIPULATION.

If someone calls or emails you asking for sensitive information, it's okay to say no. You can always call the company directly to verify credentials before giving out any information.

9:

BE SURE TO MONITOR YOUR ACCOUNTS FOR ANY SUSPICIOUS ACTIVITY.

If you see something unfamiliar, it could be a sign that you've been compromised. Report it to the provider for further assistance.

10:

GET HELP

If you have fallen victim to an online scam, virus or other internet nasty, help is always available.
For more information to help you recover, visit ***www.cyber.gov.au/report***

REPORT ONLINE CRIMES TO:
https://www.cyber.gov.au/report

REPORT SCAMS TO:
https://www.scamwatch.gov.au/report-a-scam

NSW GOVERNMENT | TAFE NSW