ONLINE CYBERSECURITY ADVICE

for all digital citizens

The internet is a shared resource, and securing it is

Our Shared Global Responsibility.

LOCK DOWN YOUR LOGIN

Your usernames and passwords are not enough to protect key accounts like email, banking and social media. Strengthen online accounts and use strong authentication tools – like biometrics, security keys or a unique, one-time code through an app on your mobile device – whenever offered.

KEEP A CLEAN MACHINE

Keep all software on internet-connected devices – including personal computers, smartphones and tablets – current to reduce risk of infection from ransomware and malware.

WHEN IN DOUBT, THROW IT OUT

Links in email, tweets, posts and online advertising are often how cybercriminals try to compromise your information. If it looks suspicious, even if you know the source, it's best to delete or, if appropriate, mark it as junk.

BACK IT UP

Protect your valuable work, music, photos and other digital information by making an electronic copy and storing it safely. If you have a copy of your data and your device falls victim to ransomware or other cyber threats, you will be able to restore the data from a backup.

OWN YOUR ONLINE PRESENCE

Set the privacy and security settings on websites to your comfort level for information sharing. It is OK to limit how and with whom you share information.

SHARE WITH CARE

Think before posting about yourself and others online. Consider what a post reveals, who might see it and how it might affect you or others.

PERSONAL INFORMATION IS LIKE MONEY. VALUE IT. PROTECT IT.

Information about you, such as purchase history or location, has value – just like money. Be thoughtful about who gets that information and how it is collected by apps, websites and all connected devices.

STOP | THINK | CONNECT™

STOPTHINKCONNECT.ORG

@STOPTHNKCONNECT **STOPTHINKCONNECT**