

CYBER SAFETY TIPS FOR FAMILIES



Criminals use home networks to
jump from one attack to the next.

10 things you can do to protect NH and your family.

Have a family secret phrase

Cybercriminals will often try to scam you by pretending to be another family member in need of money or assistance. Have a secret phrase known only to you that can be asked to validate if a family member on the phone or in email is really who they say they are. Never write your secret phrase down or put it on your computer.

Have Identity and Credit Monitoring

Almost all cyber crime perpetrated against individuals ends in some form of traditional credit fraud or identity theft. Sign up for identity monitoring and credit fraud prevention for you and all members of your family, even students! This is your last line of defense.



Approve new applications as a family

When a new application, social media site, or game comes out and a family member wants to use it, have a discussion as a family. Remember to investigate the type of data that will be shared on the program and read the developers privacy policy. Not all programs that are fun and useful are also safe.



Have Multiple Wifi Networks

Setting up two wifi networks is easy and doesn't require any additional hardware. Have one network for your work laptops and cellphones, and a different network for your kids, video games, and internet of things devices like cameras, appliances, TVs or visitors. Work devices are often infected on home networks and then infect workplaces.

Use Multi-Factor Authentication (MFA)

MFA is still one of our best defenses against compromises to our privacy. But using it at work is not enough. Multifactor Authentication is a key protection for the home as well, especially for parents and teenagers as they sign up for and use more online services than their younger siblings.



Protect your mobile devices

Keep your devices safe with biometric protections like facial recognition or fingerprint authentication. Don't plug your device into public chargers or USB ports. And make sure to update your device software often. Once updates are no longer available, that device is unsafe for continued use even if it is still in good working condition.

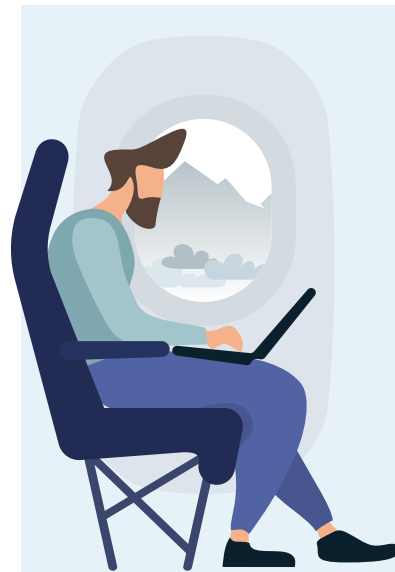


Backup your family's data to the cloud

If you are victim to a cyber attack at work, it could spread to your home and destroy your personal data too. This is just one reason to have a backup. Most online backup services are affordable and safeguard your private data and memories like photos and videos effectively. If you have a phone backup cloud, don't forget about your PC or laptop!

Social Media family rules

Social media can be great for connecting families and sharing important moments. But social media always is a place where too much information is often shared that a cyber criminal can use. Teach your family about safe social media, including not posting photos while you are away on vacation, not posting license plates or take pictures in areas that are too easy to identify.



Be safe during travel

Always limit the amount of devices you bring with you when you travel. Make sure to update all software and security settings before traveling, and remember not to use public wifi, public USB ports, or use banking, health, or work-related apps unless you are on cellular or a secure network such as a VPN, unless it has been approved by your office.

Teach and Enforce Password Hygiene

Stealing passwords is part of more than 90% of cyber crimes in NH. But it's not just parents at risk. To prepare your children to be safe online, have a family password reset day once a year and work together to teach the importance of changing passwords.



For more cyber safety resources, visit:
www.theatomgroup.com/mcdp