SECURE YOUR MOBILE LIFE

Mobile Devices are at the center of our digital lives, which makes them a target for cyber criminals.

Criminals often target NH residents using mobile devices. Mobile devices are with us all day, everyday. We've become accustomed to consuming sensitive data and having sensitive conversations using them.

8 Tips for Mobile Security:

1 Don't scan random QR codes

QR Codes aren't always bad. They are often used on brochures, menus, and advertisements in order to redirect you to a website. But many attackers publish QR codes that lead you to malicious sites that can infect your device with malware or steal data from you.

2 Don't open sensitive apps on free WiFi

Sometimes using free WiFi is unavoidable. In these cases, limit the use of your phone to non-sensitive activities and do not access applications containing personal data such as banking apps, work email, or health related apps.

3 Don't click on links in text messages

Smishing is an attack where the criminal sends you a message that appears to be legitimate and asks you to click a link. These links often lead to pages that try to harvest credentials from you or trick you into entering a username, password, or other sensitive information. Many legitimate companies don't send text messages with links!

4 Use at least an 8 digit passcode

The default on many phones requires a 4 digit passcode. We recommend using at least 8 digits and always activate biometric protections such as fingerprint or facial recognition. Biometrics are the best protection you have against unauthorized access to your device.

5 Don't use public chargers

Public chargers and USB ports, especially those in hotel rooms, should be considered dangerous. These types of chargers can be swapped out by an attacker and replaced with a cable, USB port, or charging device that records data as it leaves your phone. Whenever possible, avoid public chargers and USB ports.

6 Update your phone and apps weekly

Keeping your phone OS and apps up to date is a critical part of your mobile security. We recommend you check for updates weekly, always update your phone before travel, and if possible discontinue the use of phones that no longer support the latest software. Once a manufacturer discontinues support for a phone, it stops getting security updates as well!

7 Apps are more secure than websites!

Downloading a mobile app is often more secure than using a website version provided by the same company. Mobile Applications provide additional layers of security that safeguard data and credentials in ways not possible through regular websites. For example, if your bank has a website and a mobile app, when using your phone, use the mobile app for best security!

8 Wipe all data after 10 passcode tries

Physical security is an important part of keeping your digital life secure. Most mobile devices have a setting to erase all data after 10 failed passcode attempts. While this setting may not be ideal if you have young children who have access to your phone, it is a key protection for everyone else!

How to Report a Cyber Incident

Cyber incidents often go unreported in New Hampshire. Reporting is a critical part of safeguarding our state. It allows incident responders, law enforcement, and policy makers to see the types of cyber events happening in our state. Please consider doing your part to report any cyber incident, no matter how small it may seem at: **www.nh.gov (click on this icon at the bottom of the page)** →

NH CYBER DEFENSE PROGRAM · POWERED BY ATOM

Primex³ NH Public Risk Management Exchange

New Hampshire DoIT

The Municipal Cyber Defense Grant is a collaboration between The ATOM Group, LLC. and the The New Hampshire Department of Information Technology. It is managed in coordination with the New Hampshire Public Risk Management Exchange and serves all New Hampshire based municipal governments, schools, and public sector organizations. For more information about the MCDG Program and the free services we provide, please visit us at https://www.theatomgroup.com/mcdp.