One CREDIT UNION

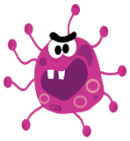
Don’t Get Burned! Put on your Sunscreen and Cyberscreen this Summer

As you consider your relaxation time this summer, make sure that you are not relaxing your vigilance when it comes to online safety for you and your family. Mobile devices, including smartphones, laptops and tablets, provide a convenient way to stay connected everywhere you go. These devices also contain a lot of information about you, your family and friends. Most mobile devices contain personal information like contacts, photos, videos, location data, account information, health and financial data. It’s important to know how to use your mobile device securely so that your information is protected. The tips below will help you achieve that goal.

1. Device Screen Lock – Locking your device with a PIN, passphrase, or biometrics can help protect your personal information and settings should your phone be lost or stolen.

TIP: Don’t use a passphrase/PIN that you already used somewhere else or a simple passphrase/PIN to protect your device. For example, using “1234”, “1111” or the word “password” are not strong enough to protect your information.

2. Install Security Software – Install Anti-Virus and Malware detection software to help protect your device from malicious applications. Malicious software can not only steal information off your device, track you, and invade your privacy but may also attempt to perform unauthorized financial transactions.



TIP: There are several free Anti-Virus and Malware detection software options listed below. Watch this to learn more about Malware: https://www.youtube.com/watch?v=XU8PHihT_P4

3. Use Secure WiFi Networks

Open public WiFi hotspots at airports, cafes, and tourist attractions are a convenience for you and hackers looking to score. Avoid doing tasks that access or expose sensitive information while on such networks. i.e. online banking, accessing other financial data or health records.

TIP: Consider installing an application that encrypts your online communications like Norton WiFi Privacy or ZoneAlarms Capsule.

4. Update Your Device – Look for and install updates for your mobile device operating system as soon as they are available. Newer versions or software patches tend to make the device more secure by correcting known security vulnerabilities in the current version.

5. Download Apps from Trusted Sources – Always download applications from trusted sources such as: Google Play, iTunes, or the App Store. Applications downloaded from sources on the internet are more likely to contain malware or other malicious code. Keep a watchful eye on apps your children may download with in app purchase to avoid unexpected expenses.

6. Application Privileges – During installation carefully review required application permissions to know what information the application can access on your device.

TIP: Always question what the application has access to on your device. Ask yourself does the free app really need to be able to read or send text messages or access my photos or camera? If not consider installing a different application.

7. Application Lock Launch Security – Use security software to set launched applications to require an additional PIN or fingerprint to open the application after the phone is unlocked.

8. Links and Attachments – Take care not to open attachments or click on links in messages you weren't expecting or from someone you don't know. Behind a link or within an attachment malicious software can wait for the unsuspecting user to interact with it so it can install on your mobile device.

9. Jail Breaking/Rooting – Jail Breaking or Rooting, which is modifying your device operating system, may provide more features, however it is a dangerous practice. Doing this will also circumvent the overall security of the device. Don't do it!

10. Usernames/Passwords –

Application usernames and or passwords should not be set to be remembered on any technology device. Also, it's best to store your username and password list in an encrypted file format or offline in a locked enclosure.

TIP: For more tips on account security visit: www.lockdownyourlogin.com

Free Mobile Device Security Software:

Norton Mobile Security – Antivirus/Malware
Malwarebytes Anti-Malware - Antivirus/Malware
McAfee Mobile Security - Antivirus/Malware
Vipre Mobile Security - Antivirus/Malware
Norton App Lock – Lock apps with additional security