CTIA
The Wireless Association®

Cybersafety

With more wireless devices than people in the U.S., we have the ability to communicate anytime, anywhere.

As our use of the devices increases and expands to new features and functions in other areas such as banking and healthcare, they may hold even more personal data.

By following CTIA–The Wireless Association® and its members' simple CYBERSAFETY tips, consumers can actively protect themselves and their data.

For more information, please visit:
www.ctia.org/cybersafety

C – **Check** to make sure the websites, downloads, SMS links, etc. are legitimate and trustworthy BEFORE you visit or add to them to your mobile device so you can avoid adware/spyware/viruses/unauthorized charges/etc. Spyware and adware may provide unauthorized access to your information, such as location, websites visited and passwords, to questionable entities. You can validate an application's usage by checking with an application store. To ensure a link is legitimate, search the entity's website and match it to the unknown URL.

Y – **Year-round,** 24/7, always use and protect your wireless device with passwords and PINs to prevent unauthorized access. Passwords/PINs should be hard to guess, changed periodically and never shared. When you aren't using your device, set its inactivity timer to a reasonably short period (i.e., 1–3 minutes).

B – **Back-up** important files from your wireless device to your personal computer or to a cloud service/application periodically in case your wireless device is compromised, lost or stolen.

E – **Examine** your monthly wireless bill to ensure there is no suspicious and unauthorized activity. Many wireless providers allow customers to check their usage 24/7 by using shortcuts on their device, calling a toll-free number or visiting their website. Contact your wireless provider for details.

R – **Read** user agreements BEFORE installing software or applications to your mobile device. Some companies may use your personal information, including location, for advertising or other uses. Unfortunately, there are some questionable companies that include spyware/malware/viruses in their software or applications.

S – **Sensitive** and personal information, such as banking or health records, should be encrypted or safeguarded with additional security features, such as Virtual Private Networks (VPN). For example, many applications stores offer encryption software that can be used to encrypt information on wireless devices.

A – **Avoid** rooting, jailbreaking or hacking your mobile device and its software as it may void your device's warranty and increase the risk of cyberthreats to a wireless device.

F – **Features** and apps that can remote lock, locate and/or erase your device should be installed and used to protect your wireless device and your personal information from unauthorized users.

E – **Enlist** your wireless provider and your local police when your wireless device is stolen. If your device is lost, ask your provider to put your account on "hold" in case you find it. In the meantime, your device is protected and you won't be responsible for charges if it turns out the lost device was stolen. The U.S. providers are creating a database designed to prevent smartphones, which their customers report as stolen, from being activated and/or provided service on the networks.

T – **Train** yourself to keep your mobile device's operating system (OS), software or apps updated to the latest version. These updates often fix problems and possible cyber vulnerabilities. You may need to restart your mobile device after the updates are installed so they are applied immediately. Many smartphones and tablets are like mini-computers so it's a good habit to develop.

Y – **You** should never alter your wireless device's unique identification numbers (i.e., International Mobile Equipment Identity (IMEI) and Electronic Serial Number (ESN)). Similar to a serial number, the wireless network authenticates each mobile device based on its unique number.

Glossary

Adware: On its own, adware is harmless software that automatically displays advertisements. Unfortunately, some bad actors may choose to integrate spyware and other privacy-invasive software in adware.

App (Application): Downloadable tools, resources, games, social networks or almost anything that adds a function or feature to a wireless device that are available for free or a fee. Some applications may also offer users the ability to purchase content or enhanced features within the application.

Cache (or Cookie): Many websites store the initial visit so that when the mobile device user visits again, the data from the same website can appear faster.

Cloud: Cloud computing allows users and enterprise companies to store and process data and deliver applications on the network. In traditional architectures, most of the data and software needed to carry out specific functions resided only on the computer or mobile device. Under cloud architectures, careful consideration is needed to ensure data and applications are protected from abuse.

Cybersecurity: Protection from unauthorized access or malicious use of information in the mobile or telecom ecosystem, which may include networks, devices, software, applications or content.

Cybersafety (for consumers): Proactively installing, using or visiting available applications, software or trustworthy content to protect or prevent unauthorized use of personal information that is stored or accessed on a mobile device.

Cybersafety (for wireless industry): Throughout the wireless industry ecosystem (networks, devices, software, apps or content creators and other platform providers), the ability to share information and tips on how to protect the industry's networks, infrastructure and customers from unauthorized access; prevent tampering with mobile devices, software, apps or content; or malicious attempts to steal or use unauthorized information. When appropriate, this may include sharing information with the government, academia and industry experts.

Cyberthreats: Potential vulnerabilities that bad actors can exploit to compromise data, extract information or interrupt services.

Encryption: Digitally scrambling information so it can be transmitted over an unsecure network. At the other end, the recipient typically uses a digital "key" to unscramble the information so it's restored to its original form.

ESN (Electronic Serial Number): A unique number placed on and within a mobile device by its manufacturer. It is used within a wireless network to identify and confirm the device. The ESN standards were defined by TR45 for AMPS, TDMA and CDMA mobile devices.

Executable scripts: Instructions that a program or operating system reads and acts on.

Hacking: Illicitly exploiting a weakness in a networked information system to access or alter data or interfere with network or device functions. A hacker may be motivated by a number of factors, such as the challenge or profit.

IMEI (International Mobile Equipment Identifier): A unique number placed on and within a mobile device by its manufacturer. It is used within a wireless network to identify and confirm the device. The IMEI standards are defined by 3GPP in Technical Standard 21.905.

Jailbreaking: Involves removing software controls imposed by the operating system by manipulating the hardware and/or software coded onto the device.

Malware: Malicious software is computer language codes created by hackers to access or alter data or interfere with network functions. It may manifest itself as worms, Trojan Horses, spyware, adware, apps, data files or web pages with executable scripts.

MIN (Mobile Identification Number): The MIN, more commonly known as a wireless phone number, uniquely identifies a wireless device on a wireless network. The MIN is dialed from other wireless or wireline networks to direct a signal to a specific wireless device. The number differs from the electronic serial number, which is the unit number assigned by a phone manufacturer. MINs and ESNs may be electronically checked to help prevent fraud.

Operating System (OS): As of July 2012, there are more than 10 wireless operating system platforms. They include: Android (Open Handset Alliance); BlackBerry OS (Research in Motion); BREW (Qualcomm); Java (Sun Microsystems); LiMo (Open Source Linux for Mobile); iOS (Apple); WebOS (HP); Windows Mobile (Microsoft); Windows Phone (Microsoft); and bada (Samsung).

PIN (Personal Identification Number): An additional security feature for wireless phones, much like a password. Programming a PIN into the wireless phone can be accomplished either through the Subscriber Information Module (SIM) or other permanent memory storage on the wireless device that requires the user to enter the access code each time the device is turned on and/or used.

Provider: Also known as a carrier, service provider or network operator, a provider is the communications company that provides service to end user customers or other carriers. Wireless carriers provide their customers with service (including air time) for their wireless phones.

Privacy Settings: Ability to determine how personally identifiable information (PII) is used by wireless applications, devices and services. Consumers should always review the privacy policy of a wireless application, device and service so they know when and how their PII will be made available to third parties such as their friends, commercial partners or the general public.

Rooting: Rooting allows a device owner to obtain full privileged control within the operating system to overcome any software parameters or other limits on the device. With this access, a hacker may alter or overwrite system protections and permissions and run special administrative applications that a regular device would not normally do. Once rooted, the device is jailbroken.

SIM (Subscriber Identity Module) Card: A small card that fits inside some wireless devices and communicates with a wireless network using a unique code. A SIM card may be removed and transferred to another wireless device.

SPAM: Unsolicited and unwanted emails or text messages sent to wireless devices. While carriers are constantly filtering their networks to stop SPAM text messages, spammers are evolving and changing their methods to try to get through. If you receive a SPAM email on your mobile device, file a complaint with the FCC. The FCC's CAN-SPAM ban only applies to "messages sent to cell phones and pagers, if the message uses an Internet address that includes an Internet domain name (usually the part of the address after the individual or electronic mailbox name and the "@" symbol)". The FCC's ban does not cover "short messages," typically sent from one mobile phone to another, that do not use an Internet address.

Smartphone: Wireless phones with advanced data features and often keyboards. What makes the phone "smart" is its ability to better manage data and access the Internet.

Spyware: A type of malware that functions without a user's knowledge or permission. Spyware frequently captures user activity and data, either storing it in obscure file locations or sending it to another location on the Internet.

Text Message (Short Message Service (SMS); Texting): Subscribers may send and receive a text, usually 160 characters or less, on their wireless devices.

Virtual Private Networks (VPN): A VPN allows a user to conduct secure transactions over a public or unsecure network. By encrypting messages sent between devices, the integrity and confidentially of the transmitted data is kept private.

Viruses: A computer virus is unwanted code that is capable of replicating and transmitting itself from one source (e.g., smartphone, tablet, computer) to another.

Last updated October 2012.