SecurityAwarenessNews

the security awareness newsletter for security aware people

Remote and Mobile Security

Smartphone Security Refresher

Security Tips for Travelers

Working From Home: Balancing Convenience and Security

Smartphone Security Refresher

Modern smartphones provide an extraordinary blend of connectivity and convenience. Within that blend is direct access to confidential information, ranging from bank accounts to social media profiles. Add work-related items to the mix and it's easy to understand why cybercriminals frequently target mobile devices.

With that important concept in mind, here's a quick refresher on how you can safeguard your handheld computer.

Beware of Malicious Apps

Malicious applications can steal data and give attackers access to private accounts. The best way to avoid them is by only installing apps from legitimate app stores and verified developers. It's also smart to occasionally review the apps installed on your phone and remove any you no longer use.

Keep It Locked

Just like a private account or desktop computer, it's important to protect your device with a strong password, code, or pattern. You can also use biometric authentication, such as facial recognition and fingerprints. Always lock your device immediately after use.

Stay Alert for Phishing Attacks

Phishing attacks are attempts by cybercriminals to steal data or money, and spread malware (malicious software). These attacks often happen via email, but are also sent through text messages that feature malicious links. Stay alert for common warning signs of phishing, such as threatening language and urgent requests.

Stay Updated

Updates are often issued to address crucial security concerns. By keeping your phone and all apps updated to their latest versions, you avoid potential threats associated with outdated software. Ideally, enable automatic updates so you never miss an important fix.

For work-issued devices, always follow policies regarding which apps you're allowed to install, when to run updates, and anything else required by your organization.

Security Tips for Travelers

Whether traveling for work or for pleasure, be sure to pack your security awareness skills along for the journey. Additional threats emerge in the physical world, requiring an additional focus for travelers. Don't leave home without paying mind to these tips and tricks for security on the go.

Enable Find My Device Services

Most modern phones offer a "find my device" service. This allows you to locate your phone via a second device. If you determine that the phone has been stolen or is not recoverable, you can use the remote-erase function to completely remove all personal information and reset the device to factory settings.

Mind Your Possessions

No one wants to lose a smartphone or have a tablet stolen while traveling. You can avoid this by never trusting strangers with your possessions. Always perform an inventory check when exiting accommodations (such as hotels) and public transportation.

Use Discretion

When in public, it's best to avoid accessing or discussing anything that may be deemed confidential. If you must, be sure no one can look over your shoulder to see your screen or overhear your conversation. This is especially important on airplanes with tight surroundings.

Have a Backup Plan

Since many unpredictable situations can arise, preparation is a traveler's best friend. Have a plan in place should you lose a device, a passport, a suitcase, a backpack, and so on. Memorize the contact information of someone you trust and research your destination before you leave.

Remember Policy

When you travel for work, it's your responsibility to know and always follow organizational policies. Those policies are designed to ensure security and privacy no matter where you go.

Working From Home:
Balancing Convenience and Security

Working from home comes with great responsibility. Not only does it require self-discipline to stay focused and on task, but it also creates additional security concerns. It is much easier for organizations to control and reduce risks when everyone works from a central location.

Therefore, it's vital for remote workers to understand their roles in this matter so they can enjoy the conveniences of working from home while prioritizing security. Here's how:

Separate Work and Personal

As a general rule, it's best to use organization-issued devices and accounts only for work purposes. For example, never use your work email for personal reasons or vice versa. This separation helps organizations maintain the confidentiality of information and helps you maintain your privacy.

Secure Your Home Network

Many routers use default usernames and passwords. It's important to update those to something unique and secure. Additionally, use a strong Wi-Fi password and keep your network gear patched and updated. For help with this, look up your equipment model online for setup and maintenance tips.

Use Virtual Private Networks

A virtual private network, or VPN, is a security tool that encrypts your internet connection. Many organizations require remote workers to use an approved VPN in order to access anything work-related. It's your responsibility to adhere to VPN requirements.

Lock Your Workstation

It's vital that no one else in your household gains access to work-related devices and information. To prevent this from happening, lock your work devices immediately when not in use, and protect them with strong passwords.

Follow Policy

Working remotely does not exempt anyone from following policies. In fact, remote work often requires enhanced policies that must be followed at all times. Circumventing them for any reason could compromise the privacy and security of everyone associated with an organization.