SecurityAwarenessNews

the security awareness newsletter for security aware people

Remote Security

Being a Human Firewall at Home

Security Awareness for Travelers

Mobile Device Security

Being a Human Firewall at Home

Human Firewall:

An individual who uses situational awareness and common sense to identify and eliminate security threats.

Working from home blends convenience for employees with security challenges for organizations. Unlike traditional work environments, home offices limit various security controls typically implemented to protect data and reduce risk. That limitation places more responsibility on remote workers, who not only must maintain productivity expectations, but also maintain a firm dedication to security awareness. With that in mind, here's how you can become a human firewall at home and secure your office-away-from-the-office:

Know and follow policy

Organizational policies are designed to protect everyone's privacy and improve overall security. Those policies still apply when you work from home. In fact, there may be additional policies that remote workers must follow. It's your responsibility to know what they are and to never circumvent them for any reason.

Click with caution

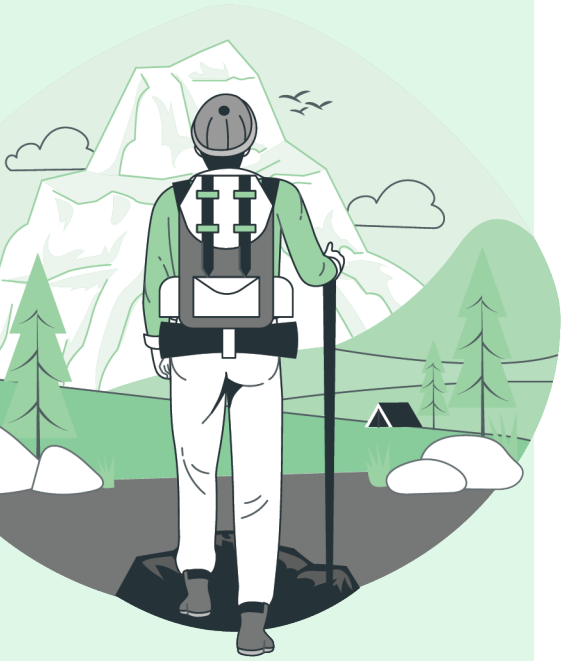
Phishing attacks don't suddenly go away when you leave the office. In fact, with so many people working remotely, cybercriminals have capitalized on new phishing opportunities (malicious video call invites, for example). Always thoroughly inspect messages and never click on a link or attachment unless you can confirm it's safe.

Protect your network

Secure your home network and WiFi with strong, unique passwords. Consider setting up a guest network for visitors, which prevents them from accessing any shared files or devices. Make sure your router is always running the latest firmware and software updates.

Separate work and personal

Don't use work devices or accounts for personal reasons. If you have approval to work on a personal computer, protect it with antivirus software and ensure it receives crucial security updates. Additionally, never let other members of your household access anything work-related.



Security Awareness for Travelers

Whether traveling for work or for pleasure, be sure to pack your security awareness skills 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.

Update before departing

Out-of-date devices and software represent security vulnerabilities. Be sure to run updates before departing and download any applications you might need for your trip. That way, you won't need to rely on potentially inconsistent data or internet connections.

Enable "find my phone" services

Most modern smartphones allow you to ping them to ring from a second device or show their location if services are enabled. This also allows you to restore your phone to factory defaults—removing all personal information—in the event that the device is lost or stolen.

Mind your things

Always keep an eye on your possessions, particularly those that contain confidential information or money. Never allow a stranger to watch your things for any reason and do an "inventory check" when deboarding 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.

Avoid public WiFi

Public networks are convenient, but they're also a major security risk. Avoid connecting to them unless absolutely necessary. If you do connect, use a virtual private network (VPN), which is software that encrypts your internet traffic and prevents others from stealing your data.

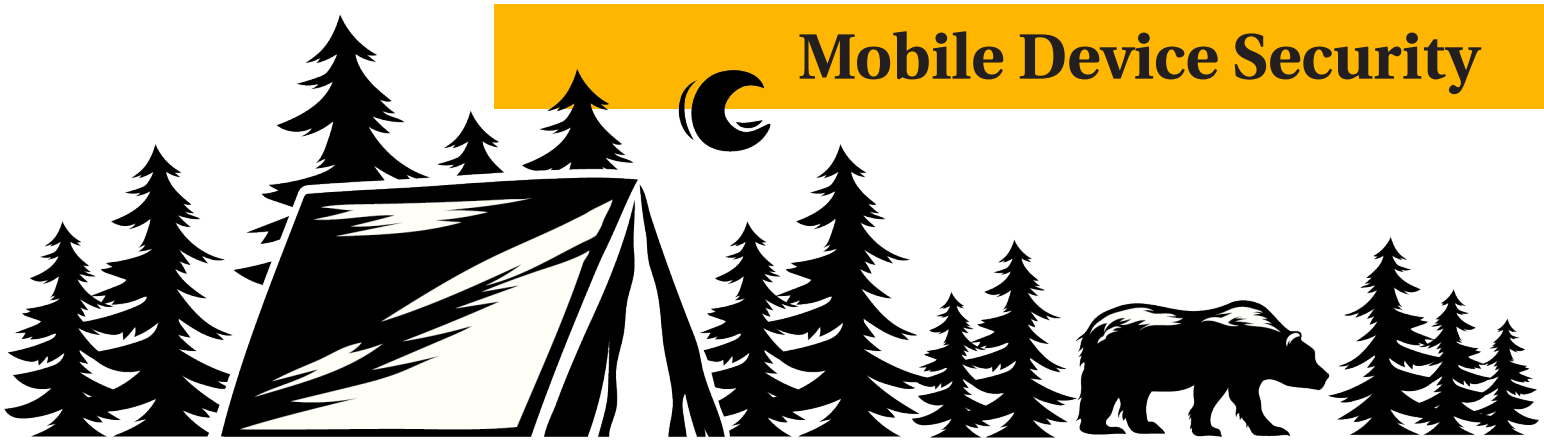
Have a backup plan

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 wallet/purse, and so on. Memorize 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 the security and privacy of data, no matter where you go. If you need more information, just ask!

Mobile Device Security



There are over four billion active smartphones in the world today. Most of them have an unprecedented amount of access to personal and professional data, including bank accounts, social media profiles, email addresses, payment services, and more.

The convenience of this access ushers in nearly endless opportunities for cybercriminals, who continue to escalate attacks on mobile devices. As such, we need to respond with equivalent measures that improve security and ensure data privacy.

We can accomplish this without sacrificing too much convenience. In fact, the path to mobile device security is a familiar one with three main areas of focus: networks, applications, and phishing.

Network security

Many devices will save and automatically reconnect to networks they've connected to in the past. This convenient feature gets abused by cybercriminals who create malicious, imposter networks designed to steal data.

If you're curious about how such an attack is possible, look up "WiFi pineapple" (a device that creates rogue access points). In the meantime, prevent your device from remembering public networks and consider disabling WiFi when not in use.

Application security

Last year alone, there were over 218 billion applications downloaded by smartphone users worldwide. You might call that a target-rich environment for scammers, who often create malicious applications that serve no purpose other than to steal information or money.

Don't get scammed. Research developers and read reviews before installing anything. After installing, limit permissions as much as possible. Many applications ask for access to text messaging, location, pictures, and so on. Only allow the minimum permissions necessary for functionality purposes.

Phishing prevention

If you check email on your phone, then you need to be alert for phishing scams, which are sometimes less obvious in mobile environments with smaller screens. Smartphones can be infected with malware, so don't click on any links or download any attachments unless you can confirm they're trustworthy.

Additionally, note that smishing attacks (phishing via text message) are becoming more and more common. They often feature warning signs similar to traditional phishing such as threatening language, a sense of urgency, poor grammar, and suspicious links. Always think before you click!

As a reminder, if you use a work-issued device, always follow policy regarding what applications you may install and what networks you may connect to.