emtrain

CYBERSECURITY 101:

PERSONAL DEVICES

Personal electronic devices provide unparalleled ease and convenience, but also account for nearly 30 percent of harmful data breaches. People often don't think of securing mobile devices as part of a comprehensive information security plan. But just the same, they use these devices to do things like send and receive work emails and attachments, read confidential reports, and communicate about sensitive issues. So what happens if your device is lost or stolen? Follow these important tips to avoid damaging and embarrassing information security breaches.

Password Protections:

At the very least, each of all personal devices should be protected with a secret password, that would be difficult for anyone to guess. A good password would involve a mix of letters, numbers, and special character. In addition to passphrases, bio-factor authentication using things like fingerprints and retina scans are very effective.
Avoid: Middle names, birthdays, Children/family members names, pet names, etc.

Theft Prevention

Always secure your physical devices. Don't leave cell phones or laptops exposed in unattended cars. Do not leave your computer unattended when working in a public space. Also, take advantage of any feature that allows you to remotely disable or wipe your device.

Keep Personal Devices Personal:

If possible, try to keep your work and personal devices separate. Often times, viruses and malware make their way onto devices by way of every-day web surfing and personal media downloads. Avoid these kinds of activities on your work devices, and similarly, avoid working on personal devices that may be infected with malware.

Pro Tip: "Man in the Middle attacks"

When working on Wi-Fi in a public space like a coffee shop, you run the risk of an eavesdropping attack, where cybercriminals spy on the information coming and going from your device.