FUNDAMENTAL 55: Computer Security

Key Takeaways:
– Teaching the role in ensuring and maintaining security
– Recognizing commonly used methods that protect software and data on corporate devices
– Evaluating the need for and approaches to ensuring security online
– Identifying the best practices necessary to ensure the physical security of commonly-used devices

Course Description
Computers do carry threats from a variety of sources, which can jeopardize the work you do and the content you create. The potential threats can be external hackers breaking into information on your computers and online accounts, or they can also involve a colleague accidentally, or intentionally, divulges sensitive information.

Security breaches are not always detectable by IT departments and because of that, it is the responsibility of both employees and the IT department to ensure there is appropriate computer security.

In the case that you disregard company security protocols, or if you cause a breach of security, there is the potential for legal consequences. Usually, this will depend on the circumstances: the type and extent of data stolen, in addition to the relevant state/provincial and federal laws. Always refer to your company’s

policies and IT department when in doubt or when you have any questions.

Typically, your company’s computer security policies will cover data involving business-related information that is saved on company equipment. It is unlikely that your company usually will protect your personal data. There are cases in which your company may provide you with one or more mobile devices to continue your work while you’re outside the office, like an FOB, thumbdrive, or smartphone. It is also possible that your company may allow you to use personal mobile devices for work or to access the company’s resources.

Consult with your company’s IT department and policies for proper compliance on acceptable data and equipment use, as well as how to deal with computer security threats that affect these devices.

Here are some common security threats:
– Disconnecting the power while or before saving
– Leaving written notes in the open
– Sharing passwords or having weak passwords
– Clicking “Reply all” in email
– Surprise hardware failure
– Theft and fraud
– Hacking
– Malware and viruses
– Power surges/outages and natural disasters
– Browsing or conducting transactions with unsecure parties on the web

Once more, refer to company’s policies and an IT department for measures to protect yourself, your customers , and your company. In the case that you detect a security breach, contact the IT department immediately.

Make an effort to always protect your desktops, laptops, portable drives and other mobile devices:
– Lock the room when possible
– Create a computer password
– Never leave USB flash drives unattended

– Only use secure, password-protected USB flash drives
– Ensure tablets and smartphones are out of sight and locked when not in use

If you are in a public place or around strangers, keep an eye on your equipment. As well, lock the screen with a password to prevent others from using your equipment in your absence.

It is common for your computer’s security is jeopardized by factors beyond your control and anticipation. Fluctuations in power often affect electronic equipment, and can cause grave, permanent damage if you do not take adequate precautions.

Consider any adverse weather conditions like floods or lightning in your area. When lightning strikes an electric pole or line, it can travel through the electrical system and damage any device that is plugged in. Excess water from rain, floods or other disasters can damage electronic equipment as well.

In some cases, power issues result from errors or problems at the power utility’s end. Nonetheless, these problems can damage your equipment, and your data.

If you want to prevent this from happening, use the correct power surge equipment at all times. Likely, your IT department will already have adequate measures in place to protect against such situations but if you are unsure, consult with them.