Data Leaks

Essentials Privacy

A data leak is the intentional or unintentional release of secure or private/ confidential information to an untrusted environment. Failure to report a leak can have severe consequences for the individual and lead to hefty fines for the company.

Ransomware

Essentials Internet

Ransomware is malware or a virus that encrypts the data on your computer or in some cases your whole network. You cannot access your files or pictures until you pay the ransom, or sometimes not even then.

Phone Locking

Essentials Mobile

Documents, memos, email, and contacts can be stolen if you leave your phone unlocked. It is important to guard the information. Always keep your phone locked when you're not using it.

Vishing

Mobile Social

Vishing is the telephone equivalent of phishing. It is described as the act of using the telephone in an attempt to scam the user into surrendering private information that will be used for identity theft.

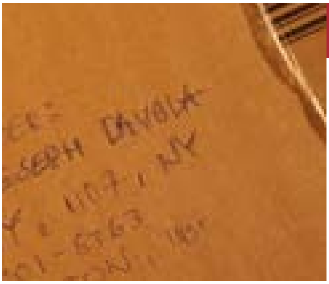
Unattended Computer

Leaving your computer unlocked and unattended can cause serious problems if someone else has access to it.

Same Password

Essentials Internet Mobile

Managing multiple passwords can be hard, but it is essential to have different passwords for different sensitive accounts.



Malicious Attachments

Email is still an important communication tool for business organizations. Attachments represent a potential security risk. They can contain malicious content, open other dangerous files, or launch applications, etc.

Removable Media

Out of office Privacy

Removable media is a common way to move larger amounts of data. The risks are numerous, including data loss, malware threats and misplacement resulting in reputational damage.

USB Key Drop

Out of Office Social Awareness

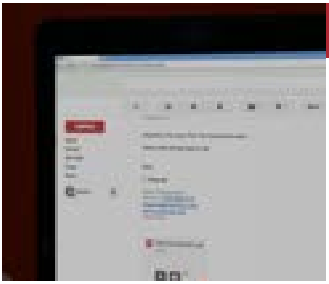
A USB key drop is when a hacker leaves a USB stick on the ground or in an open space, hoping that someone will plug it into their computer, giving access to their computer and all files they have access to on the network.

Social Engineering

Social engineering is the use of a deception to manipulate individuals into divulging confidential or personal information that may be used for fraudulent purposes often tricking people into breaking normal security procedures.

Dumpster Diving

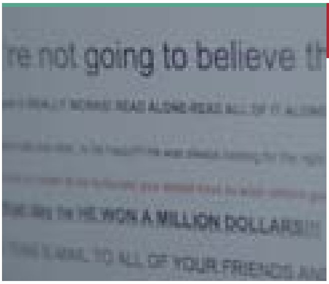
Dumpster diving is a technique to retrieve sensitive information that could be used to access a computer network. It isn't limited to searching through the trash for documents.



Spyware

Essentials Email Internet

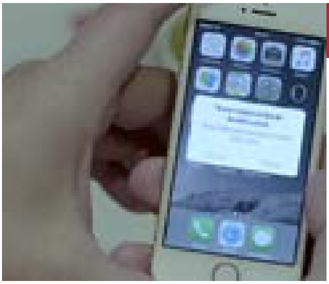
Spyware and malware are types of software that enables a hacker to obtain covert information about another's computer activities by transmitting data from the computer or


re not going to believe th
HE WON A MILLION DOLLARS!!!
TO ALL OF YOUR FRIENDS AN

Chain Mail

At the Office Email

A chain mail attempts to convince the recipient to pass it on to others. The risk is that email addresses will be distributed to a malicious person, and the email can include links to malware.



CEO Scam

Social Awareness Internet

The CEO scam is when a hacker impersonates executives and tricks employees into sending sensitive information. This includes using social engineering to manipulate people and their actions.

Clean Desk

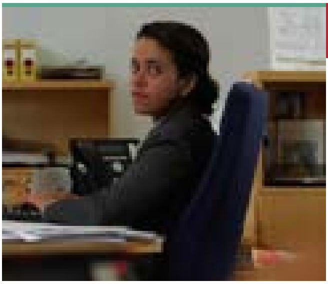
At the Office Social Awareness

Maintaining a clean desk includes not leaving sensitive documents on the desk, not writing passwords on sticky notes, cleaning sensitive information off a white board, and not leaving an access card where it might be stolen.

Computer Installs

At the Office Internet

Keep software up to date to defend against serious issues. Viruses, spyware, and other malware rely on unpatched and outdated software.



Password

Essentials

Choosing a good password is necessary. Choose one that has at least 8-10 characters and use at least one number, one uppercase letter, one lowercase letter, and one special symbol. Do not use any words that are in the dictionary.

Password Handling

Essentials

Choosing a good password is just a start. Use different passwords for different accounts and don't leave the password where it can be found. Don't send credentials by email or store them in an unsecure location.

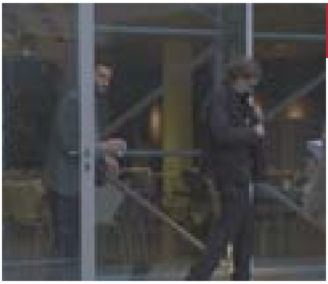
Printouts

Essentials At the Office

Printing documents and leaving them in the printer can give unauthorized persons access to confidential data.

Confidential Material

Private media is often not regulated and sometimes unsecure. Understanding the ways a hacker might gain access to unauthorized data is important.



Tailgating

Tailgating, sometimes called piggybacking, is a physical security breach where an unauthorized person follows an authorized one into a secure location.

Phishing

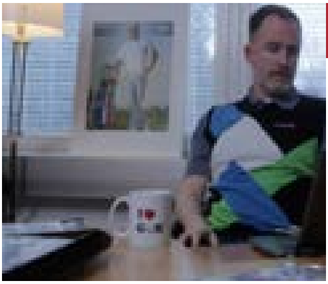
Essentials Email Social Awareness

Phishing is the fraudulent practice of sending emails purporting to be from reputable companies in order to induce individuals to reveal personal information, such as passwords and credit card numbers.

HTTPS

Essentials Email Social Awareness

Hypertext Transfer Protocol Secure (HTTPS) is a variant of the standard web transfer protocol (HTTP) that adds a layer of security to the data in transit.



Spear Phising

Spear Phishing is the practice of studying individuals and their habits, and then using that information to send specific emails from a known or trusted sender's address in order to obtain confidential information.

Shoulder Surfing

Shoulder surfing is a type of social engineering technique used to obtain information such as personal identification numbers, passwords, and other confidential data by looking over the victim's shoulder.

Free WiFi

Out of Office Internet

People usually use free WiFi without thinking. One of the most common open WiFi attacks is called a Man-in-the-Middle (MitM) attack, where a hacker can monitor all traffic and get sensitive information.

Home WiFi

Out of office Internet

Home networks are often set up in a rush to get connectivity ready as soon as possible. Most people do not take any steps to secure their home network, making them vulnerable to hackers.

Keylogger

At the Office

A keylogger is a piece of malicious software or hardware (a small device connected to the computer keyboard) that records every key-stroke you make on a keyboard.