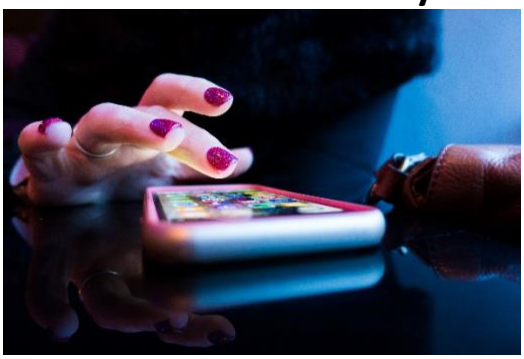
-On-device data security



Enable security features on smartphones and tablets

Specific security features vary between devices and operating systems. Use whichever features your device offers that provide the best security for your needs:

- **Password, passcode, or PIN:** Setting a password, passcode, or PIN to access your device is generally simple and effective. Use a code that is four digits or longer, and keep it secret, like you do for your email password or passphrase.
- **Unlock pattern:** Some handheld devices let you set unlock patterns that function like PINs. Use a pattern with some complexity (for example, with at least five points), keep it secret, and protect it from observers. Additionally, be aware that smudges on the face of your device may reveal your pattern to unauthorized users.
- **Device lockout:** Most handheld devices provide a lockout option that locks the device if someone makes several consecutive unsuccessful attempts to enter the password, PIN, or pattern. Using the lockout option can thwart a brute-force attempt to guess your password, PIN, or pattern. Setting the lockout limit to 10 attempts is usually sufficient.
- **Auto-wipe:** Auto-wipe is similar to the lockout option, but more secure. After several consecutive unsuccessful password, pattern, or PIN attempts, the device will automatically erase (wipe) all stored data and reset itself to the factory defaults.

  When you use the auto-wipe option, make sure to back up your data regularly (for example, to a desktop computer or a cloud storage service). Consult your device's documentation for instructions on backing up data.
- **Encryption:** Certain handheld devices are capable of employing data encryption. Consult your device's documentation or online support resources for information about available encryption options.

The following common features are frequently useful, but can also create security risks. You may want to consider disabling them:

- **Bluetooth:** Consider disabling Bluetooth connectivity on your device unless you need it. Hackers and data thieves can use Bluetooth connections to "eavesdrop" on your device and access your sensitive data.
- **GPS:** Consider disabling Global Positioning System (GPS) and other location services unless you need them. Your physical location (or the locations of your device) is a piece of sensitive data that you may not want stored or broadcast. Conversely, if your device is GPS-enabled, some apps and services (such as Find My iPhone) can help locate your device if it is lost or stolen.

-Find, Lock, or Erase a lost or stolen device

Android Devices

Find, lock, or erase a lost Android device

If you lose an Android phone or tablet, or Wear OS watch, you can find, lock, or erase it. If you've added a Google Account to your device, Find My Device is automatically turned on. Learn how to make sure that your device can be found if it gets lost.

To find, lock, or erase an Android phone, that phone must:

- Be turned on
- Be signed in to a Google Account
- Be connected to mobile data or Wi-Fi
- Be visible on Google Play
- Have Location turned on
- Have Find My Device turned on

If you used your lost phone for 2-step verification, you must have a backup phone or backup code.
Remotely find, lock, or erase

1. Go to android.com/find and sign in to your Google Account.
    - If you have more than one phone, click the lost phone at the top of the screen.
    - If your lost phone has more than one user profile, sign in with a Google Account that's on the main profile. Learn about user profiles.
2. The lost phone gets a notification.
3. On the map, you'll get info about where the phone is.
    - The location is approximate and might not be accurate.
    - If your phone can't be found, you'll see its last known location, if available.
4. Pick what you want to do. If needed, first click Enable lock & erase.
    - Play sound: Rings your phone at full volume for 5 minutes, even if it's set to silent or vibrate.
    - Secure device: Locks your phone with your PIN, pattern, or password. If you don't have a lock, you can set one. To help someone return your phone to you, you can add a message or phone number to the lock screen.
    - Erase device: Permanently deletes all data on your phone (but might not delete SD cards). After you erase, Find My Device won't work on the phone.
      Important: If you find your phone after erasing, you'll likely need your Google Account password to use it again. Learn about device protection.

Apple Devices

If your iPhone, iPad, or iPod touch is lost or stolen

If you lose your iPhone, iPad, or iPod touch or think it might be stolen, these steps might help you find it and protect your information.

If Find My [device] is enabled on your missing device

You can use the Find My app to find your device, take additional actions to help you recover it, and keep your information safe.

1. Sign in to iCloud.com/find on the web or use the Find My app on another Apple device.
2. Find your device. Open the Find My app or go to iCloud.com and click Find iPhone. Select a device to view its location on a map. If the device is nearby, you can have it play a sound to help you or someone nearby find it.
3. Mark As Lost. This will remotely lock your device with a passcode and you can display a custom message with your phone number on your missing device's Lock screen. It will also keep track of your device's location. If you added credit, debit, or prepaid cards to Apple Pay, the ability to make payments using Apple Pay on the device is suspended when you put your device in Lost Mode.
4. Report your lost or stolen device to local law enforcement. Law enforcement might request the serial number of your device. Find your device serial number.
5. If your missing device is covered by AppleCare+ with Theft and Loss, you can file a claim for your lost or stolen iPhone. Skip to step 7 below.
6. Erase your device. To prevent anyone else from accessing the data on your missing device, you can erase it remotely. When you erase your device, all of your information (including credit, debit, or prepaid cards for Apple Pay) is deleted from the device, and you won't be able to find it using the Find My app or Find iPhone on iCloud.com. After you erase a device, you can't track it. If you remove the device from your account after you erase it, Activation Lock will be turned off. This allows another person to turn on and use your device.
7. Report your lost or stolen device to your wireless carrier, so they can disable your account to prevent calls, texts, and data use. Your device might be covered under your wireless carrier plan.
8. Remove your lost or stolen device from your list of trusted devices.

If you use Family Sharing, any family member can help locate another member’s missing device. Just have your family member sign in to iCloud with their Apple ID, and you can find any device that you or your family members use with Family Sharing.

If Find My [device] isn't turned on on your missing device

If you didn't turn on Find My [device] before your device was lost or stolen, it can't be used to locate your device. But you can use these steps to help protect your data:

1. Change your Apple ID password. By changing your Apple ID password, you can prevent anyone from accessing your iCloud data or using other services (such as iMessage or iTunes) from your missing device.
2. Change the passwords for other internet accounts on your device. This can include email accounts, Facebook, or Twitter.
3. Report your lost or stolen device to local law enforcement. Law enforcement might request the serial number of your device. Find your device serial number.
4. Report your lost or stolen device to your wireless carrier. Your carrier can disable the account, preventing phone calls, texts, and data use.
5. Remove your lost or stolen device from your list of trusted devices.

Find My [device] is the only way that you can track or locate a lost or missing device. If Find My [device] isn't enabled on your device before it goes missing, there's no other Apple service that can find, track, or flag your device for you.

-Social engineering, phishing, and other malicious activities

9 Examples of Social Engineering Attacks

Examples of social engineering range from phishing attacks where victims are tricked into providing confidential information, vishing attacks where an urgent and official sounding voice mail convinces victims to act quickly or suffer severe consequences, or physical tailgating attacks that rely on trust to gain physical access to a building.

The nine most common examples of social engineering are:

1. Phishing: tactics include deceptive emails, websites, and text messages to steal information.
2. Spear Phishing: email is used to carry out targeted attacks against individuals or businesses.
3. Baiting: an online and physical social engineering attack that promises the victim a reward.
4. Malware: victims are tricked into believing that malware is installed on their computer and that if they pay, the malware will be removed.
5. Pretexting: uses false identity to trick victims into giving up information.
6. Quid Pro Quo: relies on an exchange of information or service to convince the victim to act.
7. Tailgating: relies on human trust to give the criminal physical access to a secure building or area.
8. Vishing: urgent voice mails convince victims they need to act quickly to protect themselves from arrest or other risk.
9. Water-Holing: an advanced social engineering attack that infects both a website and its visitors with malware.
   The one common thread linking these social engineering techniques is the human element. Cybercriminals know that taking advantage of human emotions is the best way to steal.
   Traditionally, companies have focused on the technical aspects of cybersecurity – but now it's time to take a people-centric approach to cyber security awareness.

How Does Social Engineering Happen?

Social engineering happens because of the human instinct of trust. Cybercriminals have learned that a carefully worded email, voicemail, or text message can convince people to transfer money, provide confidential information, or download a file that installs malware on the company network.

Consider this example of spear phishing that convinced an employee to transfer $500,000 to a foreign investor:

1. Thanks to careful spear phishing research, the cybercriminal knows the company CEO is traveling.
2. An email is sent to a company employee that looks like it came from the CEO. There is a slight discrepancy in the email address – but the spelling of the CEO's name is correct.
3. In the email, the employee is asked to help the CEO out by transferring $500,000 to a new foreign investor. The email uses urgent yet friendly language, convincing the employee that he will be helping both the CEO and the company.
4. The email stresses that the CEO would do this transfer herself but since she is travelling, she can't make the fund transfer in time to secure the foreign investment partnership.
5. Without verifying the details, the employee decides to act. He truly believes that he is helping the CEO, the company, and his colleagues by complying with the email request.
6. A few days later, the victimized employee, CEO, and company colleagues realize they have been a victim of a social engineering attack and have lost $500,000.

Examples of Social Engineering Attacks

Savvy cybercriminals know that social engineering works best when focusing on human emotion and risk. Taking advantage of human emotion is much easier than hacking a network or looking for security vulnerabilities.

These examples of social engineering emphasize how emotion is used to commit cyber-attacks:

Fear

You receive a voicemail that says you're under investigation for tax fraud and that you must call immediately to prevent arrest and criminal investigation. This social engineering attack happens during tax season when people are already stressed about their taxes. Cybercriminals prey on the stress and anxiety that comes with filing taxes and use these fear emotions to trick people into complying with the voicemail.

Greed

Imagine if you could simply transfer $10 to an investor and see this grow into $10,000 without any effort on your behalf? Cybercriminals use the basic human emotions of trust and greed to convince victims that they really can get something for nothing. A carefully worded baiting email tells victims to provide their bank account information and the funds will be transferred the same day.

Curiosity

Cybercriminals pay attention to events capturing a lot of news coverage and then take advantage of human curiosity to trick social engineering victims into acting. For example, after the second Boeing MAX8 plane crash, cybercriminals sent emails with attachments that claimed to include leaked data about the crash. In reality, the attachment installed a version of the Hworm RAT on the victim's computer.

Helpfulness

Humans want to trust and help one another. After doing research into a company, cybercriminals target two or three employees in the company with an email that looks like it comes from the targeted individuals' manager. The email asks them to send the manager the password for the accounting database – stressing that the manager needs it to make sure everyone gets paid on time. The email tone is urgent, tricking the victims into believing that they are helping out their manager by acting quickly.

Urgency

You receive an email from customer support at an online shopping website that you frequently buy from telling you that they need to confirm your credit card information to protect your account. The email language urges you to respond quickly to ensure that your credit card information isn't stolen by criminals. Without thinking twice and because you trust the online store, you send not only your credit card information but also your mailing address and phone number. A few days later, you receive a call from your credit card company telling you that your credit card has been stolen and used for thousands of dollars of fraudulent purchases.

Download the Definitive Guide to People-Centric Security Awareness to learn how focus on human emotion and risk can instill a security culture in your organization that protects against social engineering attacks.

How to Protect Against Social Engineering

"People affect security outcomes more than technology, policies or processes. The market for security awareness computer-based training (CBT) is driven by the recognition that, without perfect cybersecurity protection systems, people play a critical role in an organization's overall security and risk posture. This role is defined by inherent strengths and weaknesses: people's ability to learn and their vulnerability to error, exploitation and manipulation. End-user-focused security education and training is a rapidly growing market. Demand is fueled by the needs of security and risk management (SRM) leaders to help influence the behaviors that affect the security of employees, citizens and consumers."
*(*Gartner Magic Quadrant for Security Awareness Computer-Based Training, Joanna Huisman, 18 July 2019)

To protect against social engineering attacks requires a focus on changing behavior. When company employees understand how easy it is to be tricked or scammed by a social engineering attack, they are more likely to be vigilant and suspicious of emails, voicemails, texts, or other cyber-attack approaches.

Changing human behavior is not easy and does not happen overnight. We know from first-hand experience that the best way to instill a cyber security aware culture and to create internal cyber heroes is with a people-centric approach to security awareness training.

To effectively protect your company against social engineering requires a focus on five people-centric elements as the foundation for security awareness training:

1. High Quality Content: engages users and provides a training program that resonates and changes behavior.
2. Personalized Campaigns: provide content that employees can relate to and apply to their day-to-day.
3. Collaborative Partner: work with a partner who uses a consultative approach to understand your unique needs to deliver a custom security awareness program designed specifically for your organization.
4. Security Awareness 5-Step Framework: a training and awareness program built on a proven methodological approach to learning and changing behavior.
5. Security Awareness As A Service: provides flexibility and support to effectively deploy, measure, and report results of phishing simulations, awareness training, and campaign visibility.

How to Stay Protected Against Social Engineering

To stay protected against social engineering attacks, it's important to recognize the power of ego. Each of us wants to believe that we would never be tricked or scammed by a phishing email or other social engineering attack. However, as we know, cybercriminals rely on all aspects of human emotion and nature to subtly deceive and trick people into acting.

It's only with first-hand experience of being phished or violated by another social engineering approach that people really appreciate how social engineering works. By using a people-centric approach to security awareness training that uses phishing simulations, engaging and relevant content, and an understanding of human nature – you can stay protected against social engineering.

-Risks of public Wi-Fi

What is public Wi-Fi?

Public Wi-Fi can be found in popular public places like airports, coffee shops, malls, restaurants, and hotels — and it allows you to access the Internet for free. These "hotspots" are so widespread and common that people frequently connect to them without thinking twice. Although it sounds harmless to log on and check your social media account or browse some news articles, everyday activities that require a login — like reading e-mail or checking your bank account — could be risky business on public Wi-Fi.

What are the risks?

The problem with public Wi-Fi is that there are a tremendous number of risks that go along with these networks. While business owners may believe they're providing a valuable service to their customers, chances are the security on these networks is lax or nonexistent.

Man-in-the-Middle attacks

One of the most common threats on these networks is called a Man-in-the-Middle (MitM) attack. Essentially, a MitM attack is a form of eavesdropping. When a computer makes a connection to the Internet, data is sent from point A (computer) to point B (service/website), and vulnerabilities can allow an attacker to get in between these transmissions and "read" them. So what you thought was private no longer is.

Unencrypted networks

Encryption means that the information that is sent between your computer and the wireless router are in the form of a "secret code," so that it cannot be read by anyone who doesn't have the key to decipher the code. Most routers are shipped from the factory with encryption turned off by default, and it must be turned on when the network is set up. If an IT professional sets up the network, then chances are good that encryption has been enabled. However, there is no surefire way to tell if this has happened.

Malware distribution

Thanks to software vulnerabilities, there are also ways that attackers can slip malware onto your computer without you even knowing. A software vulnerability is a security hole or weakness found in an operating system or software program. Hackers can exploit this weakness by writing code to target a specific vulnerability, and then inject the malware onto your device.

Snooping and sniffing

Wi-Fi snooping and sniffing is what it sounds like. Cybercriminals can buy special software kits and even devices to help assist them with eavesdropping on Wi-Fi signals. This technique can allow the attackers to access everything that you are doing online — from viewing whole webpages you have visited (including any information you may have filled out while visiting that webpage) to being able to capture your login credentials, and even hijack your accounts.

Malicious hotspots

These "rogue access points" trick victims into connecting to what they think is a legitimate network because the name sounds reputable. Say you're staying at the Goodnyght Inn and want to connect to the hotel's Wi-Fi. You may think you're selecting the correct one when you click on "GoodNyte Inn," but you haven't. Instead, you've just connected to a rogue hotspot set up by cybercriminals who can now view your sensitive information.

How to stay safe on public Wi-Fi

The best way to know your information is safe while using public Wi-Fi is to use a virtual private network (VPN), like Norton Secure VPN, when surfing on your PC, Mac, smartphone or tablet. However, if you must use public Wi-Fi, follow these tips to protect your information.

Don't:

- Log into any account via an app that contains sensitive information. Go to the website instead and verify it uses HTTPS before logging in
- Leave your Wi-Fi or Bluetooth on if you are not using them
- Access websites that hold your sensitive information, such as such as financial or healthcare accounts
- Log onto a network that isn't password protected

Do:

- Disable file sharing
- Only visit sites using HTTPS
- Log out of accounts when done using them
- Use a VPN, like Norton Secure VPN, to make sure your public Wi-Fi connections are made private

-Mobile application delivery/marketplace

Apple App Store

Google Play Store

- As of 11/18/2020 the only reputable places to download and install / update apps are the Google play store for Android devices and the Apple app store for Apple devices. These stores come pre-installed.

Trademarks:
Android and Google Play are registered trademarks of Google, Inc.
Apple, iPhone, iPad, and iPod Touch are registered trademarks of Apple Inc. App Store and Apple Pay are a service mark of Apple Inc.
Norton Secure VPN is a Copyright of NortonLifeLock Inc.
Other names may be trademarks of their respective owners.