CYBER TRAINING
INSTRUCTION GUIDE

Presented By: Robertson Ryan & Associates

Contents
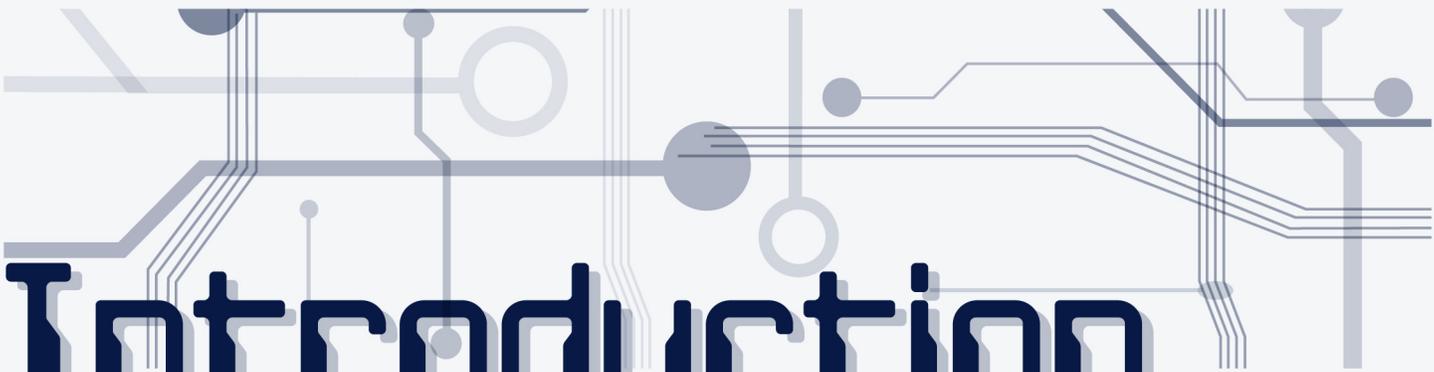
Introduction

This document is meant to supplement the Employee Cyber Training materials, and it is not meant for distribution to employees. This guide will walk you through the importance of cyber training for your employees, considerations that may be specific for your business and important topics to discuss with your employees.

As you read through this instruction guide, it is important to remember that employee cyber training should be customized to your business's unique needs and risks. For example, if your business has an online store, your risks will be substantially different than a business that only offers retail locations. Additionally, you may want to open the three employee training documents ("Overview & Best Practices," "Communication" and "Device Security") to consult as you read through this instruction guide.

Purpose

From the perspective of employees, training can often seem like one of the most monotonous tasks they can do. This is especially true when talking about cyber security, since your employees have likely been using computers, smartphones and other mobile devices for years without any negative consequences.

To ensure that employees are engaged in cyber security training, it's important to focus on the personal benefits of the training. **When employees are being trained, it's important to constantly emphasize that these measures are for both their personal and professional use.** For example, it can be difficult or next to impossible to get employees to use complicated, secure passwords to protect your business's information. However, if they learn hackers can access their personal financial accounts because they use weak passwords, and you give them tips to protect themselves, they will be much more likely to transfer those skills into a professional setting.

Training Preparation

Before training begins, it's important to read through the Cyber Employee Training Materials that you will give to your employees. As you read, be sure to familiarize yourself with all of the materials so you are prepared to answer any questions that your employees have. Also, don't be apprehensive about doing some research if you're unfamiliar with a subject—no one knows everything about cyber security.

To ensure that cyber training best fits the needs of your business and employees, you may want to focus on some topics more than others, and tailor them to your business's circumstances. For example, training could be vastly different if your business has an IT department to manage things like software updates and malware.

While you are going through the training materials, be sure to note what topics you would like to spend more or less time on. Then, by either editing the documents themselves or by taking notes, be sure to note any important steps employees need to take based on your business's unique circumstances.

The following is a general, but not comprehensive list, of the things you may want to consider including in your training documents.

QUESTIONS TO ASK BEFORE TRAINING OCCURS

Before training begins, here a few things you should consider:

- Who will be guiding the employees through the training? Does this person have a background in information technology (IT)? Does he or she have any other experience with cyber security?

- What format will be used during training (e.g., one-on-one sessions, a one-time meeting with multiple employees or weekly meetings)?

- What topics are most important to cover for your business?

- How will you know when employees have received an adequate amount of training? How will you determine that the training was effective or if more training is required?

Overview & Best Practices

SOFTWARE UPDATES

- Does your business have an IT department that will manage operating system (OS) updates and anti-virus software?

- Are your employees granted administrative permission on business devices that will allow them to update software?

- Are your employees allowed to use personal devices for business use? Do you encourage employees to regularly update these devices to get the latest security patches?

SAFE INTERNET BROWSING

- Do you specify which internet browsers your employees may use on business devices?

- Does your business block prohibited websites on business devices, or do you maintain a firewall that actively searches for vulnerabilities online and blocks employees who attempt to view them?

SECURE PASSWORDS

- Do you have criteria in place for password strength (e.g., including uppercase letters, numbers and/or special characters)?

- How often must employees change their passwords?

- Does your business have a policy regarding the use of password management systems?

NOTES: (START TYPING BELOW)

Overview & Best Practices

INSTALLING SOFTWARE

- What apps and programs are employees allowed to install on office computers? For example, can employees download and install things like Skype, Spotify, iTunes or computer games?

- Does your business's computers and other devices have guards in place to prevent employees from downloading prohibited software (e.g., not giving employees administrator privileges)?

- Are employees allowed to download apps onto mobile devices that your business owns? If so, what is the policy for purchasing these apps?

SOCIAL MEDIA

- Are employees allowed to view social media during the workday?

- Are employees allowed to view social media on business devices?

- Are employees allowed to make social media posts about work-related topics?

RECORDKEEPING

- Are employees encouraged to print important records so they can be physically stored?

- Is physical storage a priority at your business? If so, are employees encouraged to delete digital records after they have been printed?

- Does your business use a cloud storage service or remote hard drive? What is the procedure for accessing remote files? How often is the service or hard drive checked to ensure that data isn't kept for longer than it should be? Do employees have access to cloud services or remote hard drives with business information on them?

NOTES: (START TYPING BELOW)
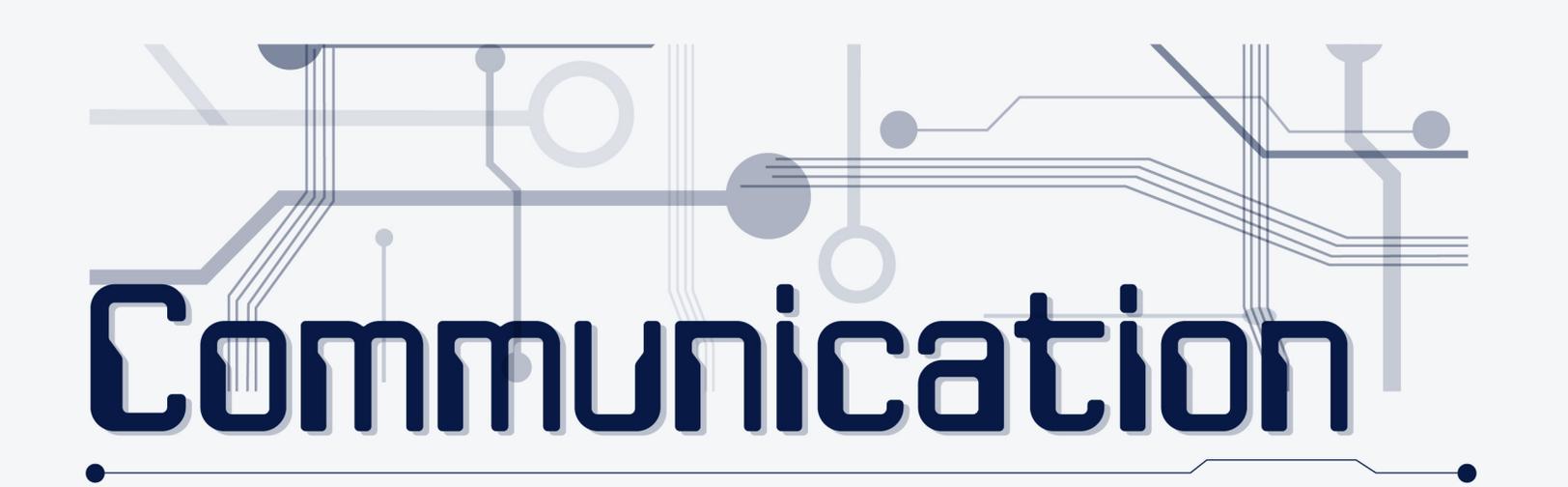
Communication

SOCIAL ENGINEERING

- Do all of your employees have access to a directory of employee information, including contact information? If so, do employees know to never share that information with anyone outside your company?

- Do employees use their personal email accounts for business use? Do you encourage employees to only use and trust work email addresses?

- Do employees know to double-check strange requests that might be part of social engineering with management first?

EMAIL

- Does your business use a unified email system? If so, does this system have a way to filter out unwanted emails, such as spam?

- Does your business have a policy for email best practices, such as verifying who sends an email and never clicking on links from an unknown source?

PHISHING AND SPEAR PHISHING

- Do your employees know not to send sensitive information electronically?

- Is your office set up in a way that employees can verify a request that's sent electronically? For example, by physically walking to a manager's office to double-check that a request is legitimate.

OTHER CYBER RISKS

- Would your employees feel comfortable approaching you or another authority figure for concerns relating to cyber security? If not, why?

- Is your business open to the public? How easy would it be for someone to walk into your office and blend in?

- Do you regularly check the credentials of people who walk into your office, or are they required to walk past a front desk?

NOTES: (START TYPING BELOW)

Device Security

WHO HAS ACCESS?

- Do your employees frequently take devices home with them? If so, do friends and family members have access to devices with business information on them?

- Do you require employees to password protect personal devices if they are used for business?

DEVICE SECURITY

- Do employees have easy access to other employees' computers or devices? If so, do you enforce a policy to lock devices when they aren't in use?

- Do you allow employees to use business devices in public areas?

- Are employees allowed to use business devices with unprotected or public Wi-Fi networks?

BUILDING SECURITY

- Do your employees know to question the presence of a stranger in the workplace?

- Are the doors and windows to your office locked, or do they require a key or password to enter?

- What are your building's operating hours? Is it possible to access the building outside these hours?

- If you have building vendors, have you contacted them to discuss any relevant cyber security provisions?

- Do you make employees aware when third-party vendors, such as maintenance and construction crews, will be at your workplace?

- Who has the keys to your office and all of its rooms? Is there a procedure to account for these keys, and to note when they're used?

NOTES: (START TYPING BELOW)

Device Security

PORTABLE MEDIA

- Does your business frequently use portable media such as hard drives, USB drives or flash drives? If so, are they password protected?

- Are employees aware that they should never plug in a portable media drive, unless they know exactly what is on it?

- Are employees allowed to bring in and use their own portable media drives?

TRAVEL

- Do your employees frequently travel with devices owned by your business?

- Are employees allowed—or even capable of using—unsecured or public Wi-Fi networks?

- Do your employees know not to leave devices in an unsecure or dangerous area? This also includes extreme temperatures, such as not leaving a laptop in a locked car on a hot or cold day.

NOTES: (START TYPING BELOW)

How to Conduct Training

Once you have determined how training will take place and gone through the training documents and tailored them to your business, you are ready to conduct training. While you are introducing employees to cyber training, you may want to bring up these topics:

- Be sure to emphasize that employees are there for their personal benefit, and that the training is intended to make their own personal information, as well as your business's, more secure.

- If you are conducting training in response to a specific incident, you may want to have a conversation with employees about the specifics regarding the incident.

- Explain to employees that the training is also meant to make sure that everyone understands your business's policies. And, even though everyone will make mistakes from time to time, employees should approach a manager or the IT department (if applicable) if they believe they or another employee has inadvertently or purposefully violated your policies.

- Encourage your employees to take notes during training.

- Be sure to ask your employees if they have any questions before training begins, and encourage them to ask questions during training. When you answer questions, it's extremely important to **be honest if you don't know the answer**. Instead, do your best to find the answer when you can, and get back to your employees as soon as you can with the answer.
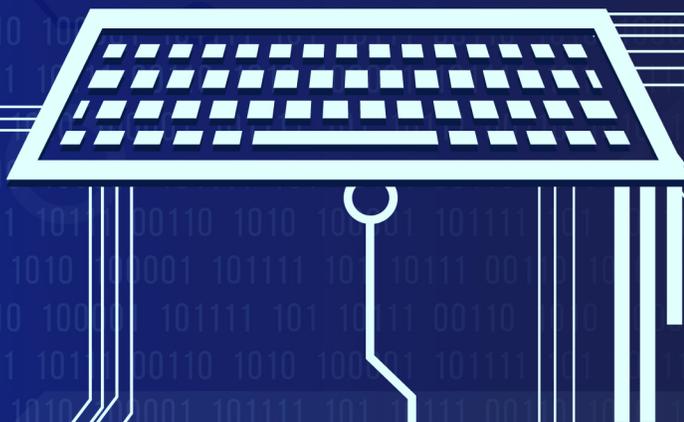
CYBER TRAINING
OVERVIEW & BEST PRACTICES

Presented By: Robertson Ryan & Associates

ROBERTSON RYAN
& ASSOCIATES
BUSINESS | PERSONAL | BENEFITS INSURANCE

Contents

Introduction

The purpose of this document is to make you aware of cyber security vulnerabilities and to give you the knowledge to protect yourself both at home and in the workplace. Although some of the topics covered in this training guide may not apply to you directly, it's important to read through them all to gain a background in cyber security procedures and the procedures that are specific to .

If you have any questions about cyber security procedures—either at home or in the workplace—contact your manager.

Software Updates
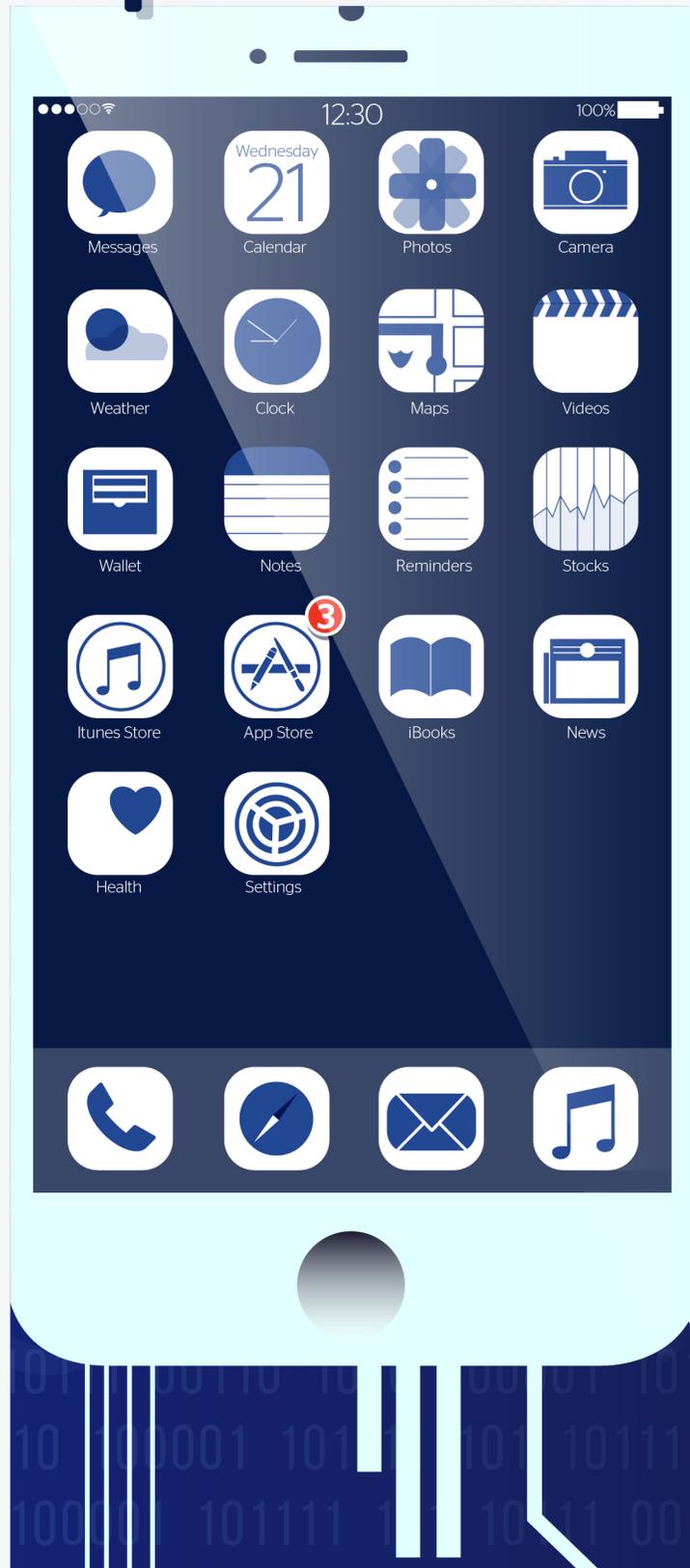
What it means: When using devices, such as laptops, desktop computers, smartphones and tablets, you may see a small window pop up on the screen asking you to update your operating system (OS) or anti-virus protection. Although these windows can be irritating and are easy to ignore, they play a critical role in cyber security.

Device manufacturers and software developers use the always connected nature of today's world to constantly adapt to new cyber threats and push updates out to their users. Companies like Apple, Microsoft and Google can respond to a hole in their software and release a "patch" to fix it within a few days. Plus, there's an added bonus for you; these patches often include new features that will make your devices more capable.

Software Updates

SIMPLE SECURITY TIPS:

- Update the software on your computer and mobile devices whenever you're prompted.
- Check your programs and applications regularly to ensure you are using the most up-to-date version. If you aren't, be sure to download updates **only** from the official developer.
- If you've installed anti-virus software, be sure to run sweeps of your device regularly to check for malware and viruses.

Making it easy: Trying to figure out how to update your device and finding a time to do it can be harder than it sounds. However, many devices now support automatic updating. This means that when you aren't likely to be using your device, such as in the middle of the night, your device will automatically download any available software updates and restart.

OPERATING SYSTEM (OS):

An operating system is the software that runs on computers, smartphones, tablets and other devices. The OS is usually updated by the device's manufacturer or software developer to fix any existing holes in security, add new features and more. Common OSs include Apple's macOS and iOS, Google's Android and Chrome OS, and Microsoft's Windows.

Safe Internet Browsing

It's easy to assume that all websites are safe to browse, especially when you're using smartphones or other mobile devices. However, malicious sites can use tactics, such as internet cookies and phishing schemes, to gain access to your device or important personal and professional information.

INTERNET COOKIE:

An internet cookie, also referred to as an HTTP cookie or simply a cookie, is a small amount of data sent by websites to your web browser, where it is then stored. Cookies enable your web browser to remember information, such as your username or browsing history, which can make it easier for you to browse online. However, other cookies can be used to track all of your browsing history or to keep track of your personal information. In the settings of your preferred web browser, there is usually an option to see and delete all of your saved cookies, which can help keep you safe as you browse online.

SIMPLE SECURITY TIPS:

- When using a web browser, check the URL for a small lock icon to be sure that a site is secure.
- Additionally, a secure website will have an "s" in the "https://" that comes before the full URL.
- Never type personal or professional information, such as usernames, passwords, telephone numbers or addresses, into a pop-up window.
- If you ever suspect that a website isn't what it seems, close your browser immediately.

PHISHING SCHEME:

Phishing is a type of cyber attack in which a hacker poses as a trusted source online in order to acquire sensitive information. This is one of the most common and technologically simple scams there is, and it can put your personal and professional information at risk.

Additionally, hackers can use personal information to make the scheme seem more legitimate. If you post information in your emails or on social media accounts, hackers can use this personal information in order to trick you into giving up more information, or information about your friends and co-workers.

Secure Passwords

Making a new password can be one of the most frustrating—and important—things you do online. Every website and service seems to have different rules about length and complexity, and you have to add your password to an ever-growing list in your memory. However, knowing the details of what goes into creating a password can give you the insight you need to make a password that's both secure and easy to remember.

WHAT HAPPENS WHEN YOU MAKE A PASSWORD?

When you make a password, the service or website that you're signing up for usually encrypts the password before storing it on its servers. That way, even if a hacker were to gain access to your password through a cyber attack, he or she still won't have access to the text that makes up your password.

Hackers can use sophisticated programs to decrypt passwords, either by trying variations of common passwords or by "brute force," where a program will try every possible combination of letters, numbers and symbols in an effort to crack your password. That's why websites often have specific password requirements.

Most Commonly Stolen Passwords

1. 123456

2. password

3. welcome
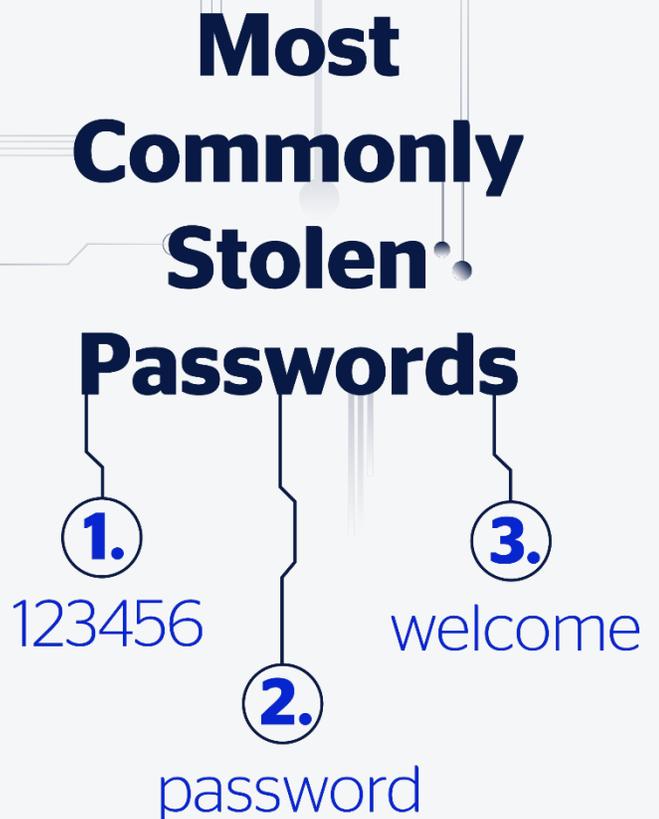
Secure Passwords

MAKING YOUR PASSWORD

However, just because passwords should be long, doesn't mean that they have to be overly complex. A long password that uses multiple words, like a short phrase, can thwart almost any attempt to crack it.

The next time you have to make a password, try typing in a favorite quote from a book, or a saying that's familiar to you. Turning a saying like "your guess is as good as mine" into "yourguessisasgoodasmine" actually makes for a strong, and in this case ironic, password.

SIMPLE SECURITY TIPS:

- Make sure that your passwords are between 8-64 characters long.
- Never keep your password written down somewhere, especially around the devices you use to access your online account.
- If you use a number of online accounts, consider using a password management tool. These websites and services require a single login, and will manage and save your passwords for you. However, be sure to research a service before you use it, as some have better reputations than others.

Most Commonly Stolen Passwords

4. master

5. 111111

6. login

Installing Software

INSTALLING SOFTWARE

Software, such as apps and computer programs, make it easy to do work and access social media and other forms of entertainment. However, hackers can use malicious software to access your messages, contacts, emails and even your location based on GPS data.

SIMPLE SECURITY TIPS:

- When you download a piece of software, make sure to check how much access it has, and that it has been made by a reputable developer. Many apps and programs ask for more access to your computer or mobile device than is required.
- Always be sure to download an app from your device manufacturer's official store. If you download something from a website or a mobile link, it is much more likely to contain malicious code.

BE CAREFUL!

Waiting...
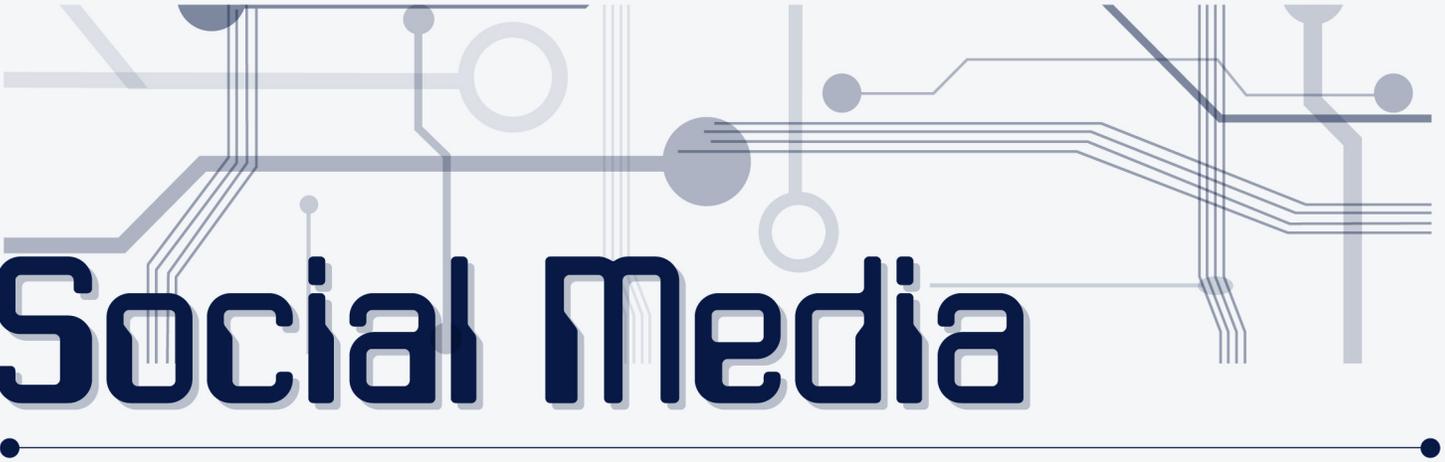
Social Media

Social media sites like Facebook, LinkedIn and Twitter allow us to easily connect with family and friends. However, they can also give hackers access to your personal information for phishing schemes. It's completely normal to check social media during the workday, but you should keep some best practices in mind.

SIMPLE SECURITY TIPS:

- Never talk about your work in social media posts without clearing it with a manager first. Even if you think something is innocent, it could give potential criminals an idea or insight into cyber attacks targeted against .
- Don't update social media when you're out of town. Although it can be tempting to post pictures and update your location for friends and family members, this will give everyone a clear picture of when you're out of the house and office. Then, anyone could use this information to steal from your home or office.
- Go into the settings of your social media accounts and check that your security settings are to your liking. Most social media sites allow you to block strangers and members of the public from viewing your information without your consent.

Recordkeeping

When it comes to things like email and electronic bills, it can be easy to shrug off things like recordkeeping. And, even though important things like receipts and account information are often stored as emails, you should take the time to think about organizing your digital information.

Additionally, you need to ensure that your data doesn't stay around longer than you want it to. Some OSs automatically save and backup your data into a cloud service to make sure it isn't accidentally deleted. If you want to delete something, you need to make sure it's also gone from the cloud and remote hard drives as well.

SIMPLE SECURITY TIPS:

- Whenever you make a large purchase or update important information online (e.g., license plate renewal or new insurance coverage), take the time to print out this information and physically store it. You should also consider locking this information away to protect it from thieves.
- Create multiple email folders to store your messages. Folders could include topics like home, work, junk and finances.
- If you need to delete digital data, ensure that it has been deleted from all cloud services and remote hard drives.

THE CLOUD:

Simply put, the cloud refers to storage on a remote hard drive. Some OSs and other cloud storage services use a large amount of protected servers to store data, such as documents, pictures and videos, to ensure that data is safe and isn't accidentally deleted.

Additionally, the cloud can refer to accessing information or devices from a distance. This can include using a remote home security system, or something as simple as accessing a picture without downloading it to your device.

Because the cloud largely exists so your files aren't accidentally deleted, you need to be sure about what cloud services you use, and that you don't keep information on them for longer than you intend. Commonly used cloud service include Apple's iCloud, Google's Drive and Microsoft's One-Drive, as well as third-party services like Dropbox and Amazon's Drive.

ROBERTSON RYAN
& ASSOCIATES
BUSINESS | PERSONAL | BENEFITS INSURANCE

CYBER TRAINING
DEVICE SECURITY

Presented By: Robertson Ryan & Associates

Contents

Introduction

It's almost impossible to find a company that doesn't utilize technology and the internet in the course of its business. Those tools make information processing and storage much easier and more efficient than they have ever been before.

The devices that we use—laptops, smartphones, tablets and more—allow us to do more business in more places around the world. However, the more we use technology, the more attractive that technology becomes to cyber criminals. In all likelihood, you have access to at least one technological device that an enterprising cyber criminal could use to harm either you or your company.

It's not really possible to avoid those risks altogether. However, it is possible to reduce the chances of falling victim to a cyber attack—if you know what to look for and what to avoid.

Introduction

This guide will cover the cyber risks posed by your devices. We'll cover a number of topics, including the following:

- Who has access to company device
- Device safety
- Building security
- Portable media
- Traveling

In this guide, we will cover some of the most common areas of cyber attacks. This training isn't intended to be exhaustive—we're only able to cover the basics in the time and space available. However, once you have a good grasp on the basics and develop a security mindset, you'll be able to apply the same set of principles to a whole host of threats

Who has access?

Company devices can contain all manner of sensitive information. Copyrighted materials, patented technologies or even private employee data may be stored on company devices.
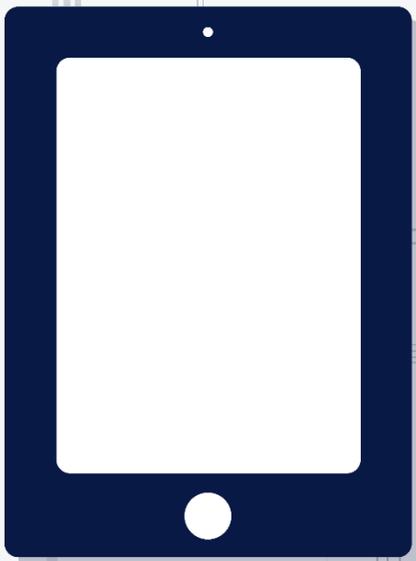
Your company may have provided you with access to the following:

- A computer
- A laptop
- A mobile phone
- A tablet

Travel

A criminal could potentially exploit any of those devices to gain unauthorized access to your company's network or its data. That's why it's important to keep tabs on who might have access to your device. That could include any of the following:

- Family
- Friends
- Co-workers
- Guests
- Vendor

Who has access?

DEVICE SECURITY

Anyone—even someone you know well and trust—could potentially use your device as a point of access for a criminal attack. Sometimes, the people you allow to use your device might actually have criminal intentions. Even if they have the best intentions, a trusted friend or co-worker could accidentally allow a hacker remote access to your device.

Keeping your devices secure doesn't mean you have to become paranoid. It just means that you need to form some good habits and follow a few simple rules:

- When you walk away from your device, make sure it's protected by bringing up the device's lock screen.
- Make sure your device is set to automatically lock after a few minutes of inactivity, in case you forget to lock it.
- Never leave your device unattended in a public place.
- Only allow others to use your device with your expressed approval and supervision.
- If you suspect someone might have used your device without your permission, or you suspect someone has done something that could put the system in jeopardy, contact your manager and/or information technology (IT) services immediately.

Building Security

Movies and television have created the image of the hacker as an individual who's sitting at a computer in a dark room, clicking on his or her keyboard. That image, however, conceals a troubling reality.
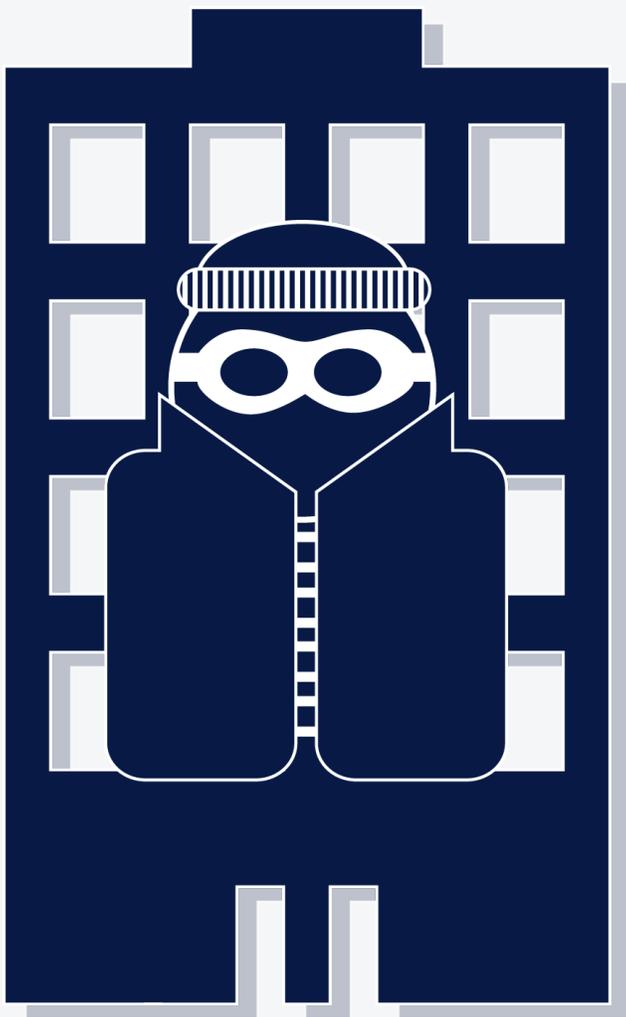
Often, hackers gain access to a system by physically breaching a company's security measures. After all, criminals are after the path of least resistance. Why write a complex computer program if the criminal can just walk up to your workstation and find your username and password written down on a notepad?

Typically, once someone has gained access to a building, he or she will be able to move around fairly freely. That's why it's important to follow these tips:

- Don't allow any unauthorized visitors into your workplace.
- If someone claims to be there to see someone, confirm with that person that he or she is expecting a guest. Make sure that the co-worker comes out to greet the guest and escorts him or her around while the guest is on-site.
- Make sure to close and lock offices, filing cabinets, lockers or anything else that could contain sensitive information.

Portable Media

Many companies and individuals store files in hosted cloud drives. However, sometimes, you may find yourself transporting files on a USB flash drive, portable hard drive or other portable media device. When doing so, make sure to keep tabs on the device.

When you're using portable media devices, follow these safety tips:

- Password protect your files.
- Store important data on separate devices. That way, if one of your portable devices is lost or stolen, whoever finds it won't have all of your important information.
- Back up your data. Just as you need to make sure you're not giving away all of your important information if you lose a CD or flash drive, you need to make sure that, if you lose a portable media device, you're not losing your only copy.
- Remove devices properly. Damaged or corrupted data can be just as costly as lost or stolen data. Remember to use the proper commands to eject flash drives or SD cards before physically removing them.

THE CLOUD:

A network of remote servers that stores a user's information. With an internet connection and the proper credentials, the user can access his or her data stored on the cloud from anywhere.
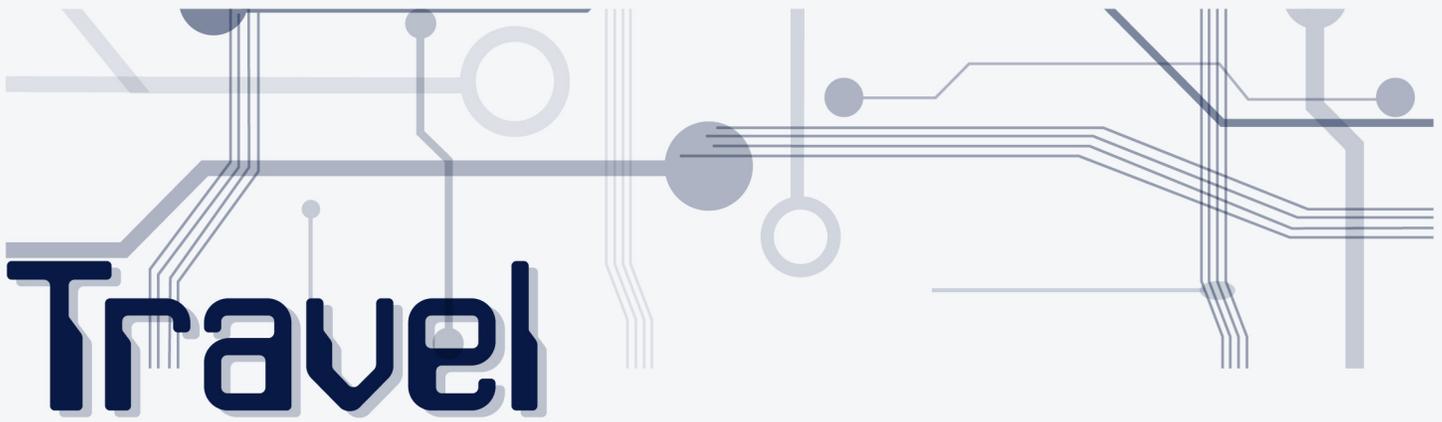
Travel

Cyber threats can always strike, but the risk can be especially high when traveling for business. Often, business travelers will have to take extra precautions when traveling. Here are some important things to remember when traveling with devices from work.

LOCK YOUR DEVICES

Lock screens ensure that unauthorized users can't access your devices. Make sure your devices are set to lock if they're inactive. That way, if you step away or accidentally leave a device somewhere, no one can use it.

INSTALL UPDATES

The software you run on your computer—especially your antivirus software and your operating system—are constantly under attack from cyber criminals. That's why the people who design that software are constantly looking for vulnerabilities and designing solutions. Before you travel, make sure you've installed all available updates.

Portable Media

AVOID PUBLIC WI-FI

Public Wi-Fi can make your life easier when you're traveling, which is something cyber criminals count on. In fact, they've been known to set up hot spots in public places like cafes, airports and hotels to try to get unsuspecting business travelers to connect. That's because, once you log on to a network, the person who set up the network or other users on the network might be able to access your device. If you're going to use a Wi-Fi network, make sure you can trust its source. Make sure the network that you access is encrypted. And, if you have to use an unencrypted public network, avoid going anywhere that will require you to enter your username and password.

TURN OFF AUTO-CONNECT FOR WI-FI AND BLUETOOTH

Phones and tablets usually have an "auto-connect" feature that will search your surroundings for available Wi-Fi networks and connect to them automatically. Likewise, most phones and tablets are able to search for Bluetooth devices and connect automatically if you wish. For all of the reasons mentioned above, it's best to disable this feature on your phone while you're traveling. That way, you'll be able to determine which networks or devices you want to connect to and which you don't.
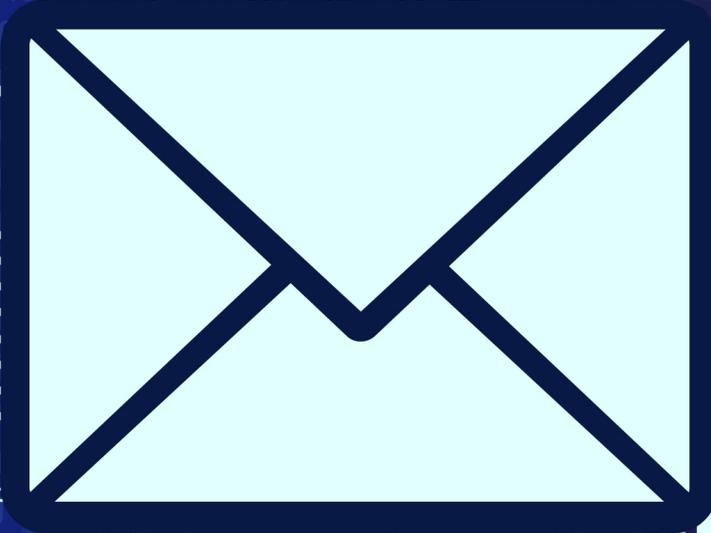
CYBER TRAINING

COMMUNICATIONS

Presented By: Robertson Ryan & Associates

Contents

Introduction

The world depends on fast, reliable communication to put businesses in touch with their employees, vendors, suppliers and, perhaps most importantly, their customers. As more consumers purchase goods online and as search engines and social media reviews drive traffic to brick-and-mortar businesses, those very channels become avenues of attack for cyber criminals.

It's not really possible to avoid those risks altogether. However, it is possible to reduce the chances of falling victim to a cyber attack—if you know what to look for and what to avoid.

Introduction

This guide will cover the cyber risks posed by communication. We'll look at a number of things, including the following:

- Social engineering
    - What is social engineering?
    - How does social engineering work?
- Staying safe with email
    - Why spam could be a problem and how to avoid it.
    - What phishing and spear phishing are and how to spot a scam.
- Social Media
    - The dangers of social media
    - Combatting social media threats
- Phone calls, face-to-face and other unexpected cyber risks
    - Analog threats in a digital world
    - Keeping the real world cyber-secure

In this guide, we hope to cover some of the most common areas of attack. Once you have a good grasp on the basics and develop a security mindset, you'll be able to apply the same set of principles to a whole host of threats.

Social Engineering

Imagine that, one day, you sit down at your computer and try to access your Facebook account. But, for some reason, you can't log in. You try to open your email, but you're being told your password is incorrect for that as well. Panic sets in as you try more social media accounts, your account for Amazon.com, and your bank accounts, but the answer is the same—you've been locked out.

Finally, you get through to a customer service representative on the phone. You explain your situation, trying to find out what happened. They begin as they normally do, by asking you security questions to verify your account—your mother's maiden name, the city where you grew up—but, inexplicably, the answers you give aren't right.

So, what happened?

WHAT IS SOCIAL ENGINEERING?

The above scenario happens more often than you might like to think, and it illustrates a principle that underlies virtually every form of cyber crime—social engineering.

Rather than attack a secure, encrypted system or database, cyber criminals use social engineering tactics to trick people into giving them access. That's why social engineering is often referred to as "people hacking."

Take the scenario above. Imagine a customer service rep for Facebook gets a frantic call about a lost password. The caller has all of the security information in hand—your mother's maiden name, your hometown, and so on—and sends an email with the

SOCIAL ENGINEERING:
Is the art of accessing information, physical places, systems, data, property or money by using psychological methods, rather than technical methods or brute force, to do so.

Social Engineering

Password reset code to the email address the caller provides.

The thing is, a hacker browsing your public Facebook page could easily find that information about you. Then, by impersonating you, a hacker could get your password reset—to an email address **the hacker** provides. And, since people often repeat the same username and password combination, that hacker could have access to many—maybe even **all**—of your accounts.

HOW DOES SOCIAL ENGINEERING WORK?

There are a number of different social engineering attacks that could affect you, and we'll mention some specific scams that you might encounter. However, there are four basic psychological tactics that are almost always at play in social engineering scams:

- **Fear of conflict.** People dislike conflict and confrontation and will use almost any excuse to avoid them. Social engineers exploit this by exuding confidence when they ask for information or physical access that they have no right to. When social engineers display confidence, most people prefer to comply with requests rather than challenge them.

- **Getting a deal.** Con artists have always relied upon the greed of their victims; social engineers exploit a similar principle. These criminals have often been known to use gifts and giveaways to get victims to let down their guard. Sometimes, the giveaway itself will be used to masquerade a piece of malicious code that the unsuspecting victim then uploads to his or her computer.

Social Engineering

- **Sympathy.** Sometimes, social engineers employ a softer tactic, using charisma and humor to gain people's sympathy or get themselves close to an individual or group. By establishing rapport and building positive feelings, victims are too distracted to realize that they're being scammed.

- **Need for closure.** The need for closure is a well-documented psychological need, and one which social engineers exploit. In the event that they ever are questioned or confronted, social engineers who've done their homework will have an answer to any challenge or question likely to come their way. In most cases, any answer—even if it's undocumented, unsubstantiated or blatantly untrue—offers people psychological closure, giving them the sense that they've done their due diligence.

HOW TO COMBAT SOCIAL ENGINEERING

Social engineering depends upon these psychological weaknesses and blind spots, but that doesn't mean you're defenseless. One big aid is simply understanding that these blind spots exist, and knowing how to recognize that you or anybody else could easily be tricked by them. However, training like this is often the best defense, because it teaches you how to recognize specific tactics and scams, and then teaches you the tactics you need to respond.

Email

Email offers people a fast way to reach out to others anywhere in the world. That's why email has become an indispensable form of communication for most businesses. However, it's for that very reason that cyber criminals see email as the perfect tool for accessing networks, gaining valuable information and launching cyber attacks.

We'll cover some important differences and distinctions when it comes to email threats, but there are three big ideas to keep in mind with all email:

1. Always verify the sender.

2. Never open suspicious attachments.

3. Never click on links if you don't trust the source.

SPAM

We use the term "spam" to refer to bulk, unwanted and unsolicited email. Spam is often thought of as the electronic equivalent of junk mail.

There's plenty of spam that's just a nuisance clogging up your inbox. However, some spam may contain attachments or links that can launch malware, spyware or other malicious code on your device. That's why it's important to take the following steps to reduce spam.

SPAM:

Bulk, unwanted and unsolicited email. Spam is often thought of as the electronic equivalent of junk mail.

Email

- **Use your spam filter.** Most email clients offer a number of filters you can use to sort email as it comes in. There's typically a "spam" or "junk" folder included. These filters have gotten much better over the years, and while a few spam emails might slip through—or a few genuine emails might be classified as "spam"— they're pretty good at keeping spam out of your inbox in the first place.

- **Flag spam when you see it.** Spam filters get better when users report spam. When a message does make its way through, take a moment to flag it as spam. You'll be doing yourself—and everyone else—a favor.

- **Be careful about giving away your email address.** Spam can't make its way to your inbox if spammers don't know where to send it. Lots of websites ask for your email address; think carefully about whether you want to give that information away. Also, be careful about posting your email address on social media sites for anyone to see.

PHISHING:
A type of cyber attack in which a hacker disguises him- or herself as a trusted source online in order to acquire sensitive information.

PHISHING AND SPEAR PHISHING

Phishing is a type of cyber attack in which a hacker poses as a trusted source online in order to acquire sensitive information. Phishing is a common and technologically simple scam that can put your co-workers and your company at risk. However, more resourceful criminals are resorting to a modified and more sophisticated technique called "spear phishing," in which they use personal information to pose as colleagues or other trusted sources.

Email

A spear phishing attack is often disguised as a message from a close friend or business partner and is more convincing than a normal phishing attempt. When messages contain personal information, they are much more difficult to identify as malicious.

Both phishing and spear phishing try to trick you into opening links that allow malicious programs onto your system or make you voluntarily give away the information that thieves want. Both kinds of attacks prey upon habit—in this case, the habit of reading the perfectly ordinary emails or text messages you receive every day. However, with a little practice, it's easy to change your habits and know when you might be looking at a phishing scam.

HOW TO AVOID BECOMING A VICTIM OF PHISHING

- **Never volunteer sensitive information.** Often, in phishing scams, criminals will impersonate a bank official, government agency or even an executive at your company and ask you to send them personal information. If an email asks you for usernames and passwords, Social Security numbers or financial account information, **STOP.** These institutions would NEVER ask you to divulge such sensitive information over an email.

- **Be suspicious of links asking for information.** If you receive an email instructing you to enter information into a website by following a link, be careful. Scammers have been known to pose as banks that ask you to "verify" your account information by signing in to what turns out to be a spoofed website. If you have any questions about your account, sign in via the links available on your bank's website—the link you usually use—and then contact customer service.

Email

- **Double-check the website's address.** Criminals have been known to purchase domains that look similar to legitimate websites, often differing by merely a letter. Make sure you're using the legitimate site before entering sensitive information.

- **Verify who you're communicating with.** If you have any doubts about an email you receive, don't hesitate to verify the information. Look up the information of the person or company who contacted you and make a phone call.

- **Trust your suspicions.** If the email asks you to do something that feels wrong or unusual, stop and think about it. Often, little things—like odd requests, careless typos or strange language—can be subtle giveaways that the person who claims to have written the email is not actually who he or she really is.

EMAIL

COMPOSE		
Inbox	**Mom**	**Are you coming to dinner? -** 6 P.M
Important	**order_confirm**	**Confirmation of order -** Order nu
Sent Mail	**FREE ITEMS**	**HELLO:) -** Gr8t to talk to u!! Pleez e-m
Drafts	**Dad**	**Resume -** Your resume looks great!
SPAM	**CONGRADULATIONS!**	**WInNeR -** Respond NoW tO ClaiM Pr
	SUPER cheap	**50% of -** Dis thee best deal 4 u. pleas
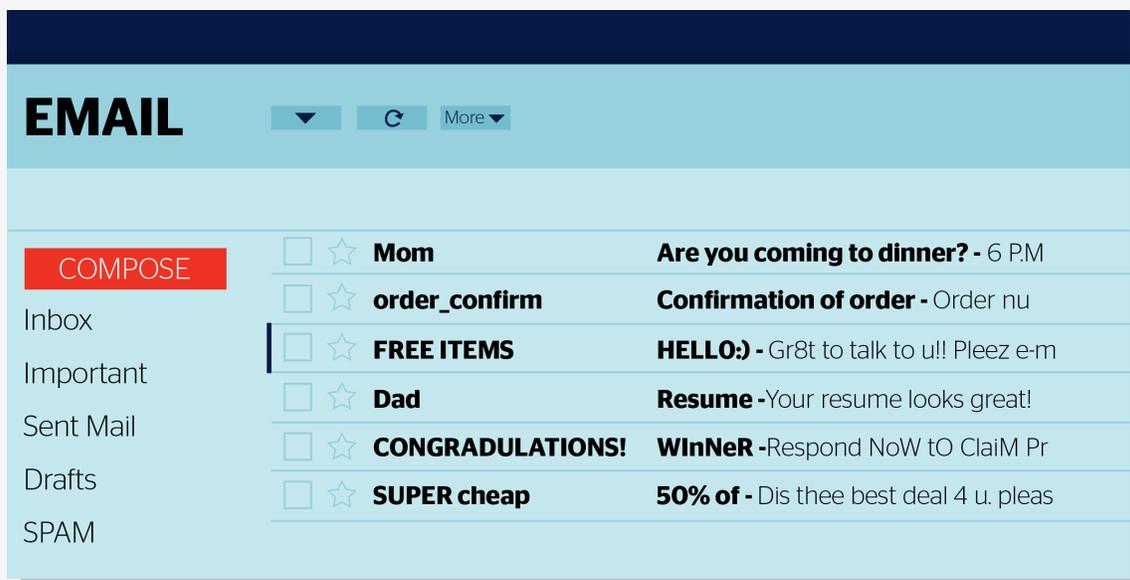
Social Media

Social media can be an invaluable tool for staying in touch with friends and family, keeping up with the news or even developing a network of professional contacts. However, the popularity of social media has made it one of the top avenues of attack for cyber criminals.

Update Status   POST

BE CAREFUL!

FAVORITES
News Feed
Messages
24 Events
Photos
Browse

PAGES
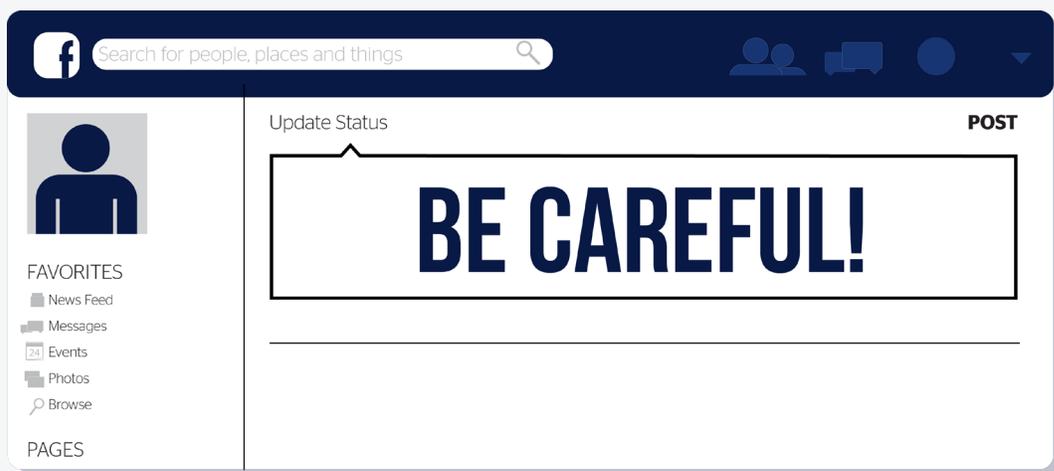
Here are just a few ways your social media accounts could put you at risk:

- **Careless posts reveal sensitive information.** Taking a picture with some co-workers and posting it to social media sounds innocent enough, but you need to be careful about what you photograph when you're at work. Things in the background could unintentionally reveal personal or proprietary information, which could allow competitors or cyber criminals unintended access to your company's intellectual property or systems.

- **Sharing information about your identity.** A few minutes on your public social media site could give anyone information about your family members, where you went to school, where you grew up, where you live, where you work and many other

Social Media

pieces of personal information. A cyber criminal can use these clues about your life to access your accounts or even steal your identity.

- **Infecting your computer with malware.** As was the case with emails, criminals have begun embedding malicious code in links on social media posts. Once the malware is on your system, criminals can use it to access your system and steal sensitive information.
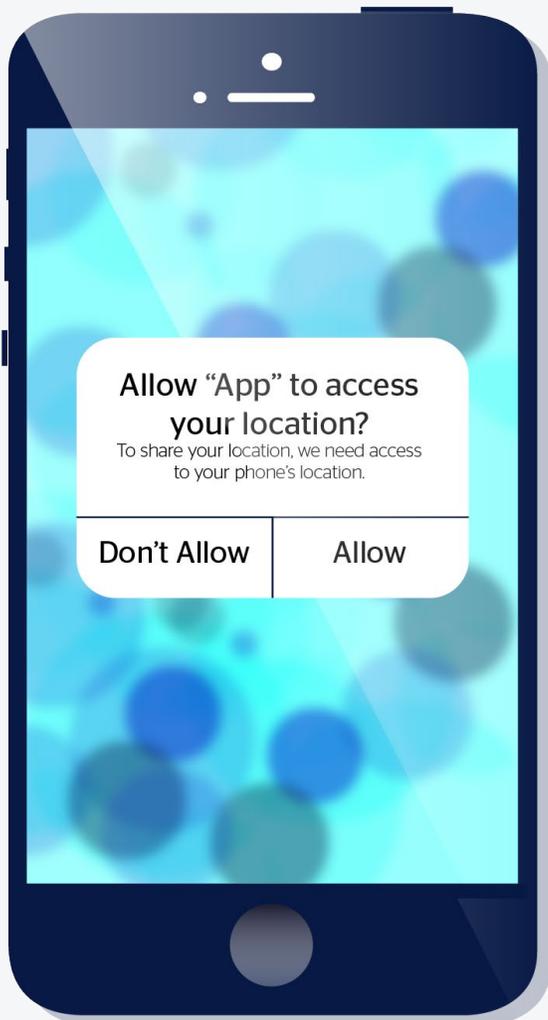
COMBATTING SOCIAL MEDIA THREATS

The same kinds of common-sense actions that you employ elsewhere on the internet can help keep you safe on social media:

- **Manage your privacy settings.** Most social media sites have some privacy controls that allow you to filter who can see your profile and what they can see when they do. Make sure you're only sharing personal information with people you know and trust.

- **Never click on suspicious links.** The same rules that apply to email and phishing scams apply here. If you're unsure about the source of the link, go directly to the company's website and search for the information you want there.

- **Think twice before posting.** Once you post to social media, the information is going to be out there forever. So, before you post, make sure that you're not sharing information that could be harmful.

Other Cyber Risks

With so much technology around us, it's no surprise that cyber crime is on the rise. However, it can be easy to forget that cyber criminals can do plenty of damage using old-fashioned technologies. In fact, phone calls and face-to-face communication are often the tools criminals use to gain access to a system.

When you're at work, keep the following tips in mind:

- **Follow company procedures.** Your company has rules about who has access to certain areas of the building or certain pieces of information. Even if it feels like a pain sometimes, follow those rules. The rules are in place to make sure that you, your company and the sensitive information at the company is only accessible to authorized persons.

- **Check credentials.** There are countless stories of criminals gaining access to computers, server rooms and locked offices simply by showing up with a uniform and a clip board. If someone shows up to your company claiming to be a vendor, repair person or police officer, don't be afraid to ask for their identification. If they're at your company for legitimate reasons, they won't mind letting you verify who they are.

- **Be careful about who you let in.** Many companies have secure doors that require a key in order to gain access. Hackers and cyber criminals have been known to linger outside of these doors, posing as an employee who forgot his or her badge, and sneak in with other employees.

- **Be careful about what you leave around your workspace.** Given the number of passwords we need to remember, it's not uncommon for employees to have them scribbled onto a note beside their workstations. If you do have to write down sensitive information, keep that information someplace secure, and make sure to shred or properly dispose of it when you're done.