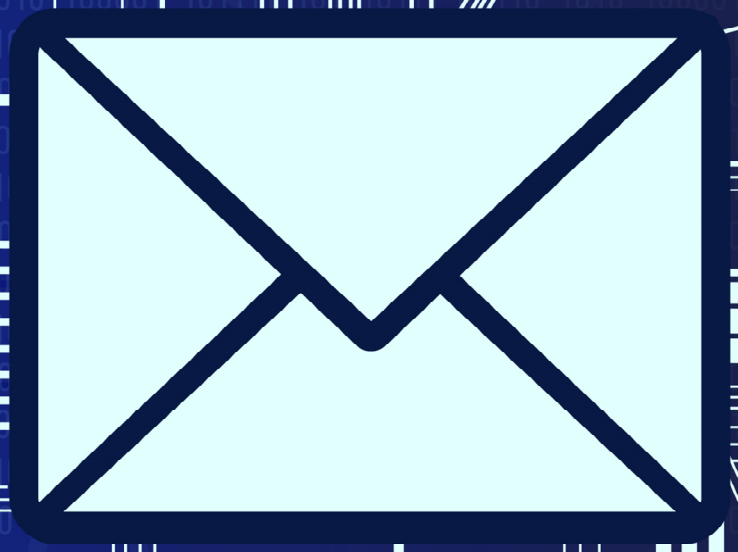
Brown & Brown

Provided By:
Brown & Brown Gulf States



CYBER TRAINING

COMMUNICATIONS

Presented By: Brown & Brown Gulf States

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.

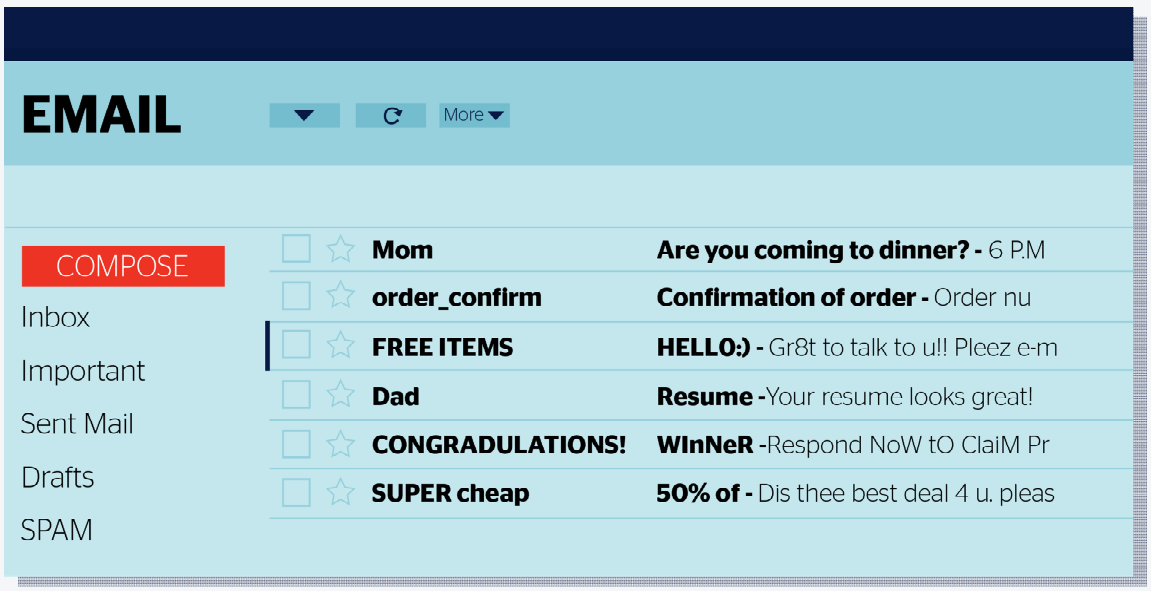
Both phishing and spear phishing try to trick you into opening links that allow malicious programs onto your system or make you voluntarily give away the information that thieves want. Both kinds of attacks prey upon habit—in this case, the habit of reading the perfectly ordinary emails or text messages 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.



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.

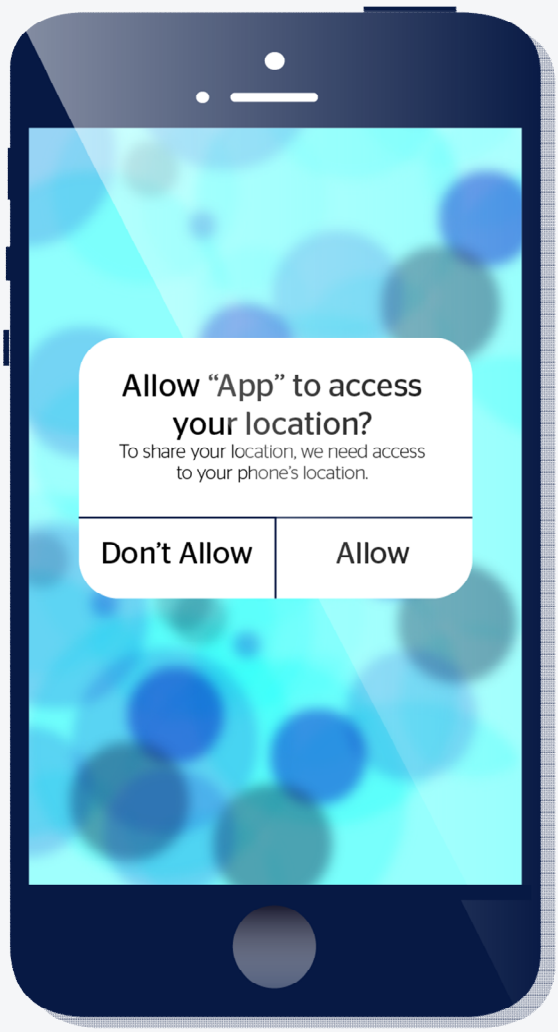
Here are just a few ways your social media accounts could put you at risk:

- 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.