THE BUSINESS GUIDE TO SECURE SOCIAL MEDIA

A plain-English, no-nonsense business owner's guide to protecting yourself and your business from social media's dark side.

We deliver technolojoy!

CONTENTS

CONTENTS

Introduction

SOCIAL MEDIA IS EVERYWHERE—AND YOU DON'T EVEN NOTICE

Everybody is on social media nowadays. You, yourself probably even have more than one account—almost anything you do, you probably post it somewhere, whether that's to your private Facebook or LinkedIn profile, or your business's Facebook, LinkedIn, Instagram or Twitter account. Most people now have more than one account for their individual use, and another few pages dedicated to their business. It's such a normal part of society in this day and age to put your profile out online, nobody thinks twice about putting all their information up for anybody to see.

Because it's become such a normal part of everyday life, I'll bet you haven't thought about the potential risks that come with putting all your information out there. Often without realizing it, we're revealing our daily routines when we post online—when we leave the house, where we get coffee, when we pack up and leave work for the day. If someone wanted to, they could figure out your every move from what you post online. Publicly or privately, it's still a danger to you and your business to have everything out there for the world to see—because if someone wants to see your page, there's always a way to hack into it or trick you into letting them view it, and then they can use that to track what you do.

This book explores the ways that cybercriminals exploit social media and rely on social engineering to negatively impact you and your business. It will examine how criminals gain access to your pages, both legally and illegally, and how they use the information they find there against you. It will also teach you how best to protect yourself while still using social media to promote your business.

Downside Of Social Media

The plain truth of the matter is that social media is absolutely necessary in this day and age. If you aren't connected on at least one platform, you might as well not exist. People rely on your social media sites to find out about your business, from what you sell to what your ethics are to who even is in charge. It's an up-to-date inside scoop all about your company, and it's pretty much the only way that anyone will bother learning about you anymore. Gone are the days of newspaper ads and phone calls; if you want to stay relevant, you have to go with the trendy social media platform of the day, or people will surely move on.

The downside of all this is that to use these sites, you have to open yourself up to a host of potential risks and dangers. It's necessary to have these accounts to keep in business, but it's exactly those things that will hook potential clients that also give cybercriminals all the information they need to do some serious damage.

So what's the solution? How do you find the middle-ground between staying relevant and protecting yourself against the threat of releasing too much information?
You may be asking:

- What can you do if someone is using your social media's information against you?
- How can you tell if your page is being exploited a cyber-criminal?
- How can you make sure you're taking the necessary steps to prevent such crimes before they happen?
- How do you keep your customers up-to-date on your business without giving away potentially dangerous information?

Social Media Horror Stories

People who don't protect their pages are currently the most at risk to having their information ending up in the wrong hands. The unfortunate thing is, a lot of people fail to take some very easy steps to make sure that they accounts are secure because they either don't know how or just don't think that they need to. Although there are a host of ways for people's personal pages to fall into a cyber-criminal's lap, this book will mainly focus on how to make sure that your small business's social media stays safe and secure.

You likely know someone who has already experienced something related to their unchecked and unprotected use of social media. Maybe they found out that someone was catfishing them; catfishing, or the use of somebody else's pictures, name, and information to fake your identity online, is more common than you would think. Or maybe they started getting unsolicited and odd messages from someone that they accepted a friend request from, even though they didn't know them.

People often leave their pages open for interaction from anybody, and don't always think about who they're talking to on the other side of the screen. If this is happening to people who aren't publicly announcing their pages, because they are just for their own private use, you can see how it's going to be a much worse problem for your business, which you're actively advertising for online.

You hear about this type of thing happening, if not through someone you know than on the news or about a friend of a friend, but you never think it's going to happen to you. Everybody thinks that they're being safe enough, that they're the exception to the rule. The reality is, if someone you know is experiencing these issues, it's likely that they're taking the same steps that you are to protect themselves, and it just isn't enough. You have to accept that you're at risk so you can start guarding yourself against invaders.

When you think about it, these are still some relatively innocuous problems, yet tons of social media users find themselves facing them every day. Imagine what could happen when that devious stranger starts to get a little bit more dangerous, and the stakes are higher because now the privacy and financial security of your business is at risk. Now you'll start to understand exactly why it's so necessary for you to take the potential threat of social media seriously. After that, you can start getting prepared to defend yourself against these problems before they ever arise.

That's where this book is going to help you. It will tell you all about the main things you should be looking out for when you're creating and using your pages online as well as what certain social media-based attacks look like so that you can recognize them before they become a serious problem for you. Once you're armed with this information, hopefully you will be better prepared in the event that you're faced with one of these situations in here.

And before you get too worried, just remember that social media is an important tool to get your business out there in the online sphere. That's where your customers are nowadays, so that's where you should be too. Just as long as you make sure you're being safe.

What This Book Will Teach You

- Post content to your social media while minimizing the danger to yourself and your business.
- Expand your privacy so that only the people you want to see your personal information can access it.
- Choose the right social media pages and keep them up-to-date and open enough to educate and appeal to your potential customer base and desired demographics.
- Learn to recognize what cyberattacks are prevalent on social media so you can see the signs before they happen to you.
- Simple, everyday steps you can take to protect your pages from posting too much or too essential information.
- Reorient your approach social media cybersecurity on a wider, more long-term scale.
- Maintain your safety in emerging and thus more dangerous social media platforms.
- Create and safeguard new social media accounts while still capitalizing on emerging platforms.
- Know what to do in the event that your page is being viewed and exploited by the wrong people.
- Maximize your scope of potential clients while minimizing the risk from potential cybercriminals.

Chapter ONE

The Plain Facts About the Use of Social Media Pages

As anyone who has been online in the past decade or even the last couple of years knows, the Internet is the number one way to advertise your business now. However, as new technologies and platforms come out what seems like every single day, it can become difficult to keep up with all of the rapid changes. Teenagers seem to be doing it with alarming ease—why can't you?

It may surprise you to learn that studies generally find that, out of all 2.8 billion people that are on social media right now, adults between the ages of 45 and 54 are the biggest users of those platforms, and they make up 21% of all the time spent on social media in total (Source: Business Insider, 2017). In this day and age, social media platforms can often be seen as a Millennial, Gen X, or Gen Z-driven phenomenon, but that's just plain not true. It's become such a central part of our society that everybody in using it.

This is why it's so crucial for people of every age to understand how best to ensure their safety online, because everyone is online. And although it can be a very useful tool for you to connect with other people, it can be a great source of trouble for you too.

Here are some basic statistics to get you started:

- According to a 2017 Business Insider report, 37% of the entirety of the world's population uses social media in some form or another.
- Nearly 70% of U.S. adults are on at least one social media site, the highest that statistic has ever been. Companies are also getting better at integrating that age group into their social media platforms in response to these numbers (Source: Business Insider, 2017)
- eMarketer reported that, in 2014, 90% of U.S. businesses were using at least one form of social media, and most of them were most invested in using social media to market to potential consumers.
- Although social media is now regarded as the single most dangerous compliance risk, one-third of the population doesn't care about strangers looking at their information on their private pages. A whopping 91% think the days of privacy are over and it's useless to even try and keep that information to yourself (Source: CSO Online, 2017)
- More than 12% of businesses have fallen victim to security breaches because of cybercrime incidents that were related to social media (Source: CSO Online, 2017)

These statistics show just how necessary it is for your business to be on social media, too, if you aren't already. Everything is online nowadays, and you're losing out on innumerable, valuable clients if you ignore certain age groups in your marketing campaigns or don't make your pages accessible to a variety of demographics. In a world where anyone can easily access anything, you should be doing all you can to garner as much attention as you can for your business. Otherwise, the public will move on.

With this, though, comes the struggle of trying to make sure that you're only attracting potential consumers without leaving yourself too vulnerable for cybercriminals to attack. When working to understand and stay up-to-date on protecting your page on emerging social media sites, you have to first figure how out how that platform works. What is the goal of the platform and how do they achieve it? Often, the goal is to get your information public so other people, whether friends or potential business contacts, can see who you are and what's going on in your life.

Spreading this kind of information can often be helpful. It can show potential employers and clients about your past work history, your work ethic, and your accomplishments or achievements. It can also give them a sense of your ethics and values. However, this same advertisement of your personal information can also leave you wide open for predators to check out everything you're doing. Before we get into direct threats, we need to get a general overview of these platforms so that we can get a better understanding of how these predators are operating within them.

Biggest Social Media Platforms Active Right Now

Name your top five favorite social networking sites that you like to use right now, off the top of your head.

All of you probably thought of a different five, didn't you? Some of you likely didn't even experience any overlap at all when thinking about the social websites that you use most.

There are a ton of social media websites out there, all of which cater to a different set of people with different sets of needs and expectations about their social networking experiences.

With an endless amount of options out there, you can pretty much guarantee that no matter what you want to see online, who you want to connect with, and what you want to do with your page, you can probably find some platform somewhere on the internet that will cater to your exact specifications. This is great for you, as a business owner, because you can get on social media and still feel comfortable with the site that you choose.

Some platforms seem to appeal to a wide range of people though, so we're going to focus on those for the sake of addressing the biggest concerns out there right now. However, all social media sites harbor the same basic risks and rewards when it comes to putting out your information online. The big websites do this especially.

For example, according to DreamGrow, who laud themselves as a "source of content marketing and social media information," Facebook, Youtube, Instagram, and Twitter are the biggest social networking sites online right now. They are closely followed by Reddit and Pinterest, and all of the aforementioned websites have over 100 million users on them as of November last year; the top three have over 800 million on each site alone. According to a survey by Forbes in 2017, there are almost two billion people on Facebook alone.

As platforms grow and they become normal parts of your day, you may be more likely to trust the other users on the website and friend or follow them even if they don't look familiar to you. You become desensitized to the dangers the more you feel that you know how to use the website. With more users, however, these sites will also have a larger amount of cybercriminals lurking on them who could potentially prey on your pages and the information that you put up on them.

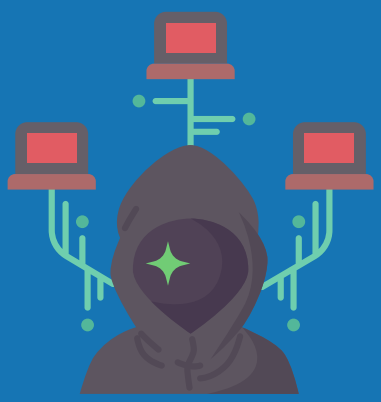
Biggest Attacks on Social Media

As platforms and the businesses on them both grow, so do the number of possible attacks a cybercriminal could launch against you. As protections shift and evolve, the cyberattacks do too. Unfortunately, there is no realistic way to outrun every single cyberattack that you may encounter now and forever, because these criminals are changing their techniques almost as fast as we develop ways to stop them in their tracks.

So, what can we do?

Instead of trying to figure out exactly how to stop each and every possible cyberattack that you may encounter, it's better for your business if you focus on making your pages as generally safe as you can, to keep out the biggest number of threats that you can. Don't worry yourself to death over the specifics. First, however, we need an understanding of just what kind of cyberattacks are big right now so that we can figure out how to prevent them on the widest possible scale.

Malware is the first and foremost thing you should be worried about when it comes to compromising your business's security. Malware is any software that gets installed onto your devices (such as your phones, computers, etc.) with the intention of damaging your computer, your files, or your business's network system. Cybercriminals will often try to get your information from your personal pages and then create personalized links that you will be more likely to click on, since they have been tailor-made for your interests. Once you do, they will then automatically and secretly install malware onto that device.



Similar to this type of attack are phishing scams, which are carried out in a very similar fashion to malware attacks. Phishing is any type of attack where the cybercriminal steals your private information by tricking you or somebody else into giving it to them, often through spam that you click on or through theft of your account information which then allows them to access your pages. Phishing attacks may involve strategies like clickjacking, wherein the hacker layers an invisible page over the website that you are on that allows them to record the information that you enter, such as your credit card information or your passwords. You never even know that they're gathering it, and suddenly your account is in danger.

By making you more likely to click on these types of links or enter this information, those criminals have a much higher chance of getting into your network and compromising your business in that way. You have to be careful about any suspicious links or messages that you might get from your coworkers, clients, employees, or other business associates that seem suspect or seem to be asking you to give up too much of your personal information that they would not normally ask for. That may indicate that they themselves have been compromised by a cyberattack in some manner and are potentially having their account used as a gateway to infect other networks and devices.

You should also watch out for distributed denial-of-service, or DDOS, attacks. A DDOS attack is when a hacker gets into your systems and inhibits you and other administrators from getting into your network. This can be for a short- or long-term prevention of access, but either way it hurts your business because it halts productivity until you fix the problem. It also gets more complicated if the hacker is using this type of attack to steal files while you're locked out or if they demand pay for the return of your administrative privileges.

Ransomware is exactly that. It forces victims to pay a fee online to get access to their systems or so that they can get their stolen data back after their information has already been taken advantage of. In most cases, it's wise to report this type of attack rather than giving in to it, especially because this is a popular way that cybercriminals attempt to get money or steal your credit card information.

You should also be wary of any site, whether it belongs to a client or business partner or any other trusted individual, that appears to offer or require third-party updates to your computer or that offers free goods or services to anyone who clicks a link, takes a survey, or otherwise interacts with a program or website that you do not already know. Although it would be ideal to get free things just for filling out a survey or being the thousandth person to visit a website, it's not realistic to expect that type of good luck.

There is no real way to completely remove yourself from all the cyberattacks going on within social media. Someone you know will likely fall victim to it, and you will probably encounter websites that try to lure you into giving up your personal information. What you can do, however, is make yourself aware of the big attacks that you should be watching out for, so that you can prepare yourself and know what to do when the time comes to avoid it and protect yourself accordingly.

Chapter TWO

Understanding the Practicality of Social Media

The way that you establish your business online is a big part of how potential consumers perceive your organization, especially because your website and social media pages are likely how they are encountering your company for the very first time. It's the first impression they have of you. If they don't like anything from the way you tag to what you post, it's not difficult for customers to leave comments, replies, and reviews about your business. Although these can be very beneficial because good reviews are basically free promotion, anyone who accesses your pages can also instantly see any negative comments that have been left about you.

When you start thinking about all the different ways that having social media can harm you, you might become inclined to think that you're better off without it. If you don't establish yourself on multiple different platforms, then you don't have to worry about keeping them all up to date, relevant, and safe; you don't have to make sure they're all individually protected; and you can be absolutely guaranteed that cybercriminals won't be coming after you, because you have nothing for them to look at anyway.

The reality is that this is just not realistic. A lot of business these days goes on online; that's where you have to advertise to garner consumer attention, and that's where a lot of clients will find you when they're looking up good places to take their business.

Being online benefits you, too. You can more easily conduct background checks on potential employees, so that you can identify possible issues before you even hire them. That alone might help you choose between two equally qualified candidates. Social media helps you get to know your employees before you hire them, so that you can see whether their personality and personal ethics adhere to your business model, will coexist well with the employees you already have and convey the public persona you've cultivated for your business.

Social media also helps you monitor your competition. You can instantly know about a competitors latest successes, what their prices are and who they do business with; it's also a good way for you to see their reviews and adjust your own business practices accordingly, depending on what customers liked or disliked about their experience at your own and others' places of business.

You can also make contacts and build your business more easily via the internet; networking has never been easier than when you can do it from home or right out of your workplace. You can advertise more easily too, by posting up your services and publishing press releases or other information online. It's fast, easy, and widely accessible to anyone who wants to look you up or whom you want to attract.

If you're not easily identifiable online—meaning if potential customers can't easily find a location, phone number, and/or customer service representative for you—they're very likely to just take their business elsewhere instead of going through the trouble to research you further. Nowadays, clients like ease and transparency. People are much less likely to just wander around town looking for a good place to take their business, and happen into your shop to see if you suit their needs. They research the closest, highest quality, most affordable, and overall best place to take their business needs before actually coming in to do business with you. So if you're not online, you might as well not exist.

It’s not just the online market making social media a necessity nowadays. It’s actually really beneficial to your business if you establish yourself online in a clear, open way.
Consumers don’t want to work hard to figure out how you can help them. They want to know immediately if you fit their needs or not. Advertising yourself well is important. Let them know on the first page whether or not you’re going to do what they want.If you make your services clear and your locations and hours obvious and accommodating, they’re much more likely to pick your company for whatever job they want done. On top of that, it’s a good idea to have some employees on your pages too. Clients want an easy way to get in contact with you to ask about your business and services, whether that’s by calling a customer service line, or communicating through a chat function with a representative.

Also, look professional but be clear. Clients don’t want to be searching through links upon links to figure out what they’re looking for. If your LinkedIn connects to your Instagram which connects to your Twitter which connects to your Facebook, they already gave up three links ago. It’s good to advertise your different social media accounts on one another’s pages so that customers can find exactly what information they want without searching too hard, but don’t make it a maze to get the answers to their questions. You already got them on your page, and that’s the real challenge. Now you just have to keep them there.

Keeping Your Business Relevant in the Age of Social Media

There is more to using social media to benefit your business than simply choosing a couple of platforms and making yourself prominent on there. You also need to make sure that you are choosing the correct platforms to advertise yourself on so that you can attract the highest number of people from all demographics onto your webpages. Choosing obscure social media to use just won't cut it; it doesn't matter if you're the most-visited page on a site if that site is totally obscure and has a very low traffic count overall, even if it fits the exact specifications that you were looking for in a profile. You have to bend to accommodate the consumer.

Instead, you should focus on building a following on relevant pages. Sadly, there is no simple answer to this. Establishing yourself on the current big social media platforms of the day won't ensure that you stay relevant forever. As times change, new platforms are invented, and old ones fall out of style, you need to keep up to date by making sure that you are constantly aware of the big, popular platforms and not paying as much attention to your accounts on the ones falling by the wayside. If, to use a very outdated example, you're paying more attention to your MySpace account than your Facebook page, you have definitely become irrelevant with current social media trends and the modern Internet user.

This is why we're going to focus on choosing the right pages to expend effort on. Although, like I already said, websites fall in and out of style quickly, we're going to focus for the sake of this book on the ones that are popular this year and have been enjoying steady, if not increasing, fame for a while.

Facebook

Facebook is the number one social media platform in the modern age, and it's been enjoying that title basically uncontested since MySpace ended in 2009. According to Forbes, it is now home to over 50 million businesses, and Facebook itself has reported that those pages in total garner over 2.5 billion comments in a month.

This site is probably the number one way that clients follow you or check out your information to see what kind of promotions you post, the location of your business, customer service phone numbers, and other important information in a place where it is all helpfully consolidated on one page. One of the benefits of Facebook, aside from an easy access to highly relevant information, is that they can easily Like your business's page and get updates about your promotions and other noteworthy posts such as new hires, awards, products and other accolades, so it's a great place to advertise. If you're not using Facebook, you're way behind in the game – but it's never too late to get started.

YouTube

Although you may be less familiar with the idea of using YouTube as a platform to enhance and expand your business, some small business owners find it a useful tool to help them engage with their clients. Being able to show a video of what you're doing or "how to's" makes it easier to give potential clients an idea of how you do your work without them having to come in and ask questions, and that may be a point of appeal for certain people. Showing videos of events you're hosting, customer satisfaction reviews, and other videos like that is a useful marketing tool depending on what type of business you run, and YouTube gives you an advantage in this area that the other popular social media can't offer.

A report from Forbes last year found that you are better off being on some kind of video platform than not, although of course whether or not you choose to use YouTube as that platform of choice is entirely up to you. Other places that run on video include apps like Periscope, and Instagram now lets you post videos to your feed as well. Marketing campaigns especially benefit from these types of platforms, because you can show viewers exactly how to use your goods or services and explain what you can offer to them. Videos are a very good source for relaying information.

Instagram

Speaking of Instagram, this is a great platform for users to get a more visual experience with your business. You can post photographs about events and sale items you have going on, promote your goods and services, and engage your followers to send in pictures of themselves enjoying the products and services your business offers.

This site is already being used by 70.7% of businesses, according to a 2017 Sprout Social report. Over half of all users are between 18 and 29, making it a great platform on which to expand your appeal to the under-30s demographic and get support from these younger consumers. With Instagram's growing popularity and bigger base of users, it's a smart idea to get on this platform as well and further expand how you're marketing and operating your business.

Twitter

Twitter lets you talk about whatever you want in 140 characters or less. Although you may think that this makes it an unworthy platform for a business to use, because you can't convey as much information at once, Omnicore Agency reports that over 300 million people are using this site as of 2017, and that alone makes it a very valuable asset and terrific communication vehicle for you and your company

According to Brandwatch, 65.8% of businesses in the United States that have over 100 employees are on Twitter, and most people on Twitter follow an average of five businesses. Considering the vast number of people who are on here, this gives your business a good chance of being followed by a good number of people if you promote yourself right and intelligently set up your Twitter page. By using tweets to promote new products, services and sales, release new information about achievements by employees and officers, and publicly support causes that align with your business's message, Twitter can be a great place to expand your business on the web.

Websites like the ones mentioned above are just the most popular ones on the web right now, but you are by no means limited to using only these platforms. As I mentioned before, there are an endless amount of social media sites to choose from, and only you can make the call about what specific platform is going to be the best choice for your individual business.

For example, consider your intended demographic. Research indicates that younger people, for example, are more likely to do social networking online and be on very specific platforms that cater to a younger audience. In contrast, according to Business Insider, 45% of adults making over $75,000 annually are on LinkedIn right now. It's important that, whoever your intended demographic, you understand where they are and why, so that you can then use that information to your advantage.

You, as the business owner, especially need to understand how social media works and whether or not you're doing well on the ones you already have established pages on. It's not enough to expect someone else to understand your page, or to just hope that it will work out because you have a fairly steady customer base offline already. Understanding whether your company is doing well online can determine how you're going to improve how you're using these platforms, and that can only lead to profit.

You need to be keeping tabs on your business, both in the real world and online, because nobody has as much invested in your success as you do.

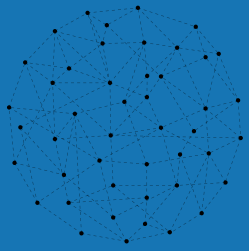
Unsecure Extensions and Why We Use Them

Although it can seem overwhelming at first, after a while you start to get comfortable with having different social media accounts. That's when you start to look for shortcuts to make achieving what you want easier, or ways that you can manage all your different pages faster and simpler.

With how much we use social media nowadays, it's not a surprise that we've become more lax about how we use them. The more these types of websites have become a normal part of our everyday lives, the more we want to make them an easier and more entertaining experience for us.

This is where a lot of the danger comes in for people and their business. You may want to enhance or simplify your experience with Facebook, Instagram or one of the other platforms you use because it makes accessing and managing your page easier, or because it's just a better experience when you add on enhancements for your computer or phone to do this.

Nowadays, there are an infinite amount of apps that are meant to enhance and simplify your social media presence. Facebook Messenger lets you use their chat function without having to actually open your Facebook account and thus clog your browser tabs with unnecessary pages. Unlike your desktop, if you're on your phone, you have to use Facebook Messenger in order to chat with someone on their platform.



Other platforms have extensions or auxiliary apps as well. There are a ton of photo apps that let you adjust, combine, or otherwise edit your pictures before posting them directly to Instagram. You can upgrade your Snapchat with extra filters or personalized emoji's and geotags. However you want to upgrade your social media experience, there's an app for that.

The problem with all these apps is that they are usually extremely unsecure. Some apps, like Facebook Messenger for your desktop, outright tell you that they aren't completely safe and secure when you try to download them. Others don't tell you, but they are transporting your information through an unsecure third-party, so you can guarantee there's a lot you don't know about who has your information now, how they use it, who they sell it to, etc. Consider the recent congressional hearings with Facebook founder Mark Zuckerberg. He outright said Facebook owned all of your data and was selling your information.

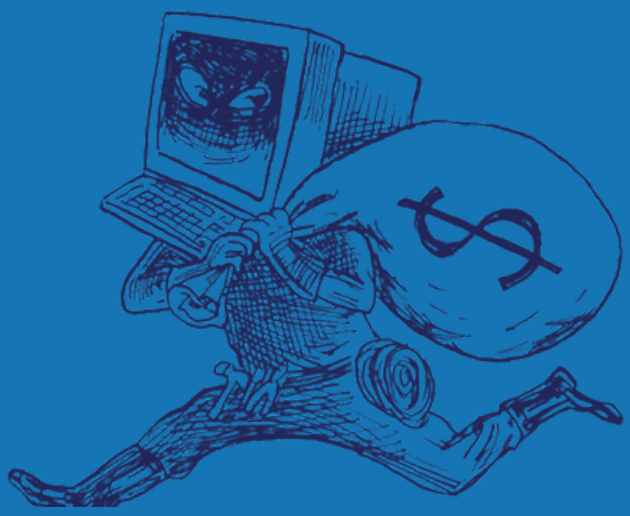
Some apps, for example, will offer to save information like your name, address, and credit card so that it's easier to use their services in the future. All you have to do is make one click, and you're done. You don't have to take out your card every time you want to make a purchase through your bank app, and you don't have to be exposing your information to anyone looking over your shoulder if you're paying on-the-go.

The danger there that you might not be thinking about, however, lays in whoever is behind the screen that can access all that information saved on their databases whenever they want. Your information isn't just in their hands, but in the hands of whoever is managing their security; one breach and your information is out there for anyone to see. Uber, for example, was just revealed to have experienced a breach like this in 2016, where nearly 60 million people had their data stolen. When apps that hold your credit card, name, and information get hacked into, it's just as dangerous as if your own network experienced a breach.

This is why it's important to just think about what you're downloading or using before you do it. Although some people heed these notices that apps and extensions give out about the ways you may be compromising your information, of course, plenty of us choose to ignore these warnings, explicit or not, and use those extensions and apps anyway because it's just more convenient to be able to text your employees without having to leave the important work page you were reading. Sometimes it's just that everyone else is using these types of supplementary apps, so it's easier if you do too. Plus, you figure that if everyone is doing it, it can't really be all that dangerous.

Obviously if this type of behavior is already ingrained into your everyday routine, you're not going to be willing to give it up easily. Although it's wise to give them up completely and just stick to the social media you know will protect your information, at the very least make sure you know who's taking possession of your information and data before you use new extensions like the ones mentioned above.

What's the takeaway? Just be vigilant. You're naturally going to be inclined to make using your social media easier the longer that you are online, and in some ways this is very helpful. Understanding just how your extensions and apps can also hurt you, however, is a critical step to ensuring the safety of your business. If it's giving someone too much information or access to your data, it may be time to delete it.



Chapter THREE

The Big Threats Going on Today

The biggest attacks that people are experiencing nowadays happen because hackers rely on one simple truth; people will behave today as they behaved yesterday, and tomorrow they'll behave as they do today. Because we have socially engineered ourselves this way, hackers exploit these tendencies and use us to infiltrate our own systems. We've wired ourselves to make them difficult to fend off and hard to get rid of once they've infiltrated your network. They might just be difficult to detect, so a lot of people who don't know the dangers that are out there online tend to fall for those particular tricks most easily—the old scam of a Nigerian prince needing your help might come to mind here, although now everyone knows that that is obviously a ploy. Cybercriminals are getting craftier instead to keeping tricking their victims in new and inventive ways. Cyberattacks are difficult to deal with simply because they're preying on our behaviors, and multiplying and evolving faster than our combative technology can keep up with as they adapt to new norms in user behavior made easy to recognize with big data, so they're always a few steps ahead. For these reasons they're just plain hard to see for the scams that they are.

Whatever the cause for a particular threat's proliferation, there are a few things that you can do to make sure that you don't become another victim. The best protection you can give your network and your business is learning to recognize which threats are most prevalent on the social media platforms that you use, so that you can be better prepared to avoid them when the time comes that you do have to face them.

THere, I'm going to teach you what the biggest threats are on the most popular social media websites, so that you won't fall victim to them when the time comes.

Let's start with Facebook, since we've already established that it's one of the most popular, if not the most popular social media platform out there right now. One trick that cybercriminals love playing is using Facebook chat to their advantage. You might think you're safe if you're only talking to people that you know in real life on your Facebook account, or replying to customers' questions and concerns through chat. But this isn't necessarily true; if the person you're talking to falls victim to a cyberattack, and you engage with them on Messenger thinking that you're talking to someone legitimate, you may be more likely to click on links they send you or give them information that you think they can be trusted with. If their account is compromised, yours is now vulnerable too if any of their messages contain phishing applications or schemes, where they were going in with the intent to steal your information. This is especially risky for business accounts that may contain a lot of sensitive information about your company.

This problem isn't limited to phishing either. Cybercriminals also tend to use this same method to forward malware to different accounts. You may see someone you follow or friended start to post links that don't seem like something they would post, or send you private messages with something you have to click on. If a friend is starting to spread suspicious-looking messages that don't look like something they would normally say or do, it's best to just ignore it and scroll right past their suspicious posts. Better yet, call them or email them and let them know you think their account was compromised. It's very likely some kind of malware that an infected account is trying to spread to your own, and once it's in your computer, they can reach any other computer on your network or spread it further to the rest of your friends' list.

Other social media pages with similar messaging and posting features might experience outbreaks of similar cybercriminal activity. Facebook is particularly noted for it, but you should be careful whenever you're interacting with someone's account when they seem to be acting out of the ordinary.

More insidious is the vast amounts of personal data these platforms store, and how easy it is to harvest it.
In early 2018, news broke about the data company Cambridge Analytica. They used an app that was built for Facebook that asked users a series of personal questions about themselves, their friends and how they interacted online. The app, when installed required users grant them permission to access their account and network. With only a few hundred thousand users downloading and using the app, it exploited the networks interrelationships, which is what makes it such a strong social media platform, to steal the personal data of some 50,000,000 people who never downloaded it and never gave them permission to harvest their data.

While what Cambridge Analytica did wasn't criminal, it demonstrates the significant exposure of personal information a simple app has access to. Moreover, cybercriminals today are already using these apps. You don't hear about them because, unlike Cambridge they don't sell the data commercially, they traffic it on the Dark Web.

Cybercriminals are getting good at personalizing their attacks for each individual platform for which their attacks are specialized. Twitter has a different interface than Facebook, and so the cyberattacks that are targeted at Twitter users are necessarily different than those that are meant for Facebook, and also different than the ones meant for Instagram, and so on.

Twitter doesn't have as big a focus on messaging as Facebook does, so instead of posing as different Twitter accounts to try and get you to divulge your information, cybercriminals might instead put out scams that offer free vouchers, or ask you to take a survey, or something similar. The goal there isn't to get you to interact with another business you think is familiar or an employee's or client's account.

Instead, they try to pull you in by offering you deals that are personalized to attract you as a business owner. The fact that it seems so tailored to your interests make it seem legitimate, but in reality this is just cybercriminals getting smarter.

Twitter has become a hotbed for spear-phishing because you do the work for the criminals; instead of having to make malware that appeals to a wide audience, they only have to get one person to fall for it. Once you're infected, it spreads to all of your contacts and anyone else you may have interacted with online; that includes your customers, too. Tripwire reported that only 30% of spear-phishing emails are opened, so you may wonder how it becomes so prevalent. The fact is that only 30% of them need to be opened. Once it's on someone's computer, their account spreads it to everyone else. 66% of spear-phishing posts, even ones that are very similar to those emails that you just ignored from a stranger, get clicked on from trusted social media pages. Just because you're smart enough to ignore traps from strangers doesn't mean you're prepared to be suspicious of pages that you know and trust.

Instagram experiences similar issues as Twitter. Spam and bot accounts will try to get you to follow them, likely to try and lure you into clicking on any of the virus-spreading links that they often post in their bio or as the caption underneath their pictures. Make sure you're only following people you know and trust not to be fake accounts, and be careful of any links that take you outside of the site.

These are potentially dangerous and could contain malware that you do not want spreading to your phone or computer.

LinkedIn scams take a different approach than luring you in by using a trusted user's page. Instead, they are aimed at installing malware into your network by directing you to outside sources. Since LinkedIn is a platform that is primarily used to view others' pages, the goal of the cybercriminals is to get you to click on a link that appears to go to someone's page or another business's profile, but instead redirects you to an entirely different page, where they then automatically install malware onto your computer —often, in the background without you even knowing that anything installed onto your computer at all.

LinkedIn is also dangerous because it's a place that is designed for you to put tons of personal information on there so that potential businesses and clients can easily find and get in contact with you. Cybercriminals are using LinkedIn as the information trove that it is and compiling lists of all the employee email accounts that are listed on the site for a particular organization. They then send an email to all of these accounts, a message that contains malware but is so tailor-made for that specific company that employees are much more likely to trust it and open the infected link. Oftentimes these emails are even signed off by a URL that appears to be from your organization, making it much more devious. Be careful of even trustworthy-seeming links and users.

Venmo is another unsafe place to conduct business operations. Venmo is a useful money-transferring apps, where you can pour funds from your bank account directly into the app and transfer it to someone else's account, as long as they also have Venmo downloaded. This is becoming a more and more popular app, as people are getting less used to carrying cash and more used to spending on-the-go. Some businesses don't take a certain type of credit card, so Venmo is a nice compromise.

It's very useful for businesses because they can still make a sale if that's the preferred payment method of the customer or they just don't have any other money on them. If they weren't intending on spending money that day, they usually still have their phone on them and thus can still make the purchase.

The danger here, though, might be obvious: You're linking your bank account, which is obviously full of important confidential information, to a much less secure and much more easily-accessible app, and then linking that to a number of other accounts that may or may not be trustworthy. Venmo makes it very difficult to view others' accounts, and you can't see their personal information, so it's hard to assess which ones are real and which are fake accounts designed to dupe you. On top of that, it sometimes takes multiple days to actually put the transaction through to your bank account, so it may seem like a legitimate transfer only for you to find out that you've been swindled once it's far too late.

There's also the trouble with what happens if Venmo gets hacked, as that would put all of your bank information at risk. Although the app itself is mostly secure, it has been hacked before. People have had their money stolen and transferred to strange accounts. After they're inside, cybercriminals can change your password and steal your money, and it's difficult to correct that. Make sure you're monitoring your account and adding all the additional safety measures you can to ensure that, if the app does get hacked, you know immediately and can quickly take steps to correct whatever happens. We'll discuss later in this book how to make your money transferring apps, including Venmo, more secure, so that you can protect these accounts and hopefully avoid any repercussions from a cyberattack at all.

Clickjacking is also a major problem across all social media platforms. Clickjacking is a type of cyberattack where cybercriminals layer an invisible screen over a web browser, so that they can record all of the keystrokes you make on that page. They often do this as a sneaky way to steal your passwords and other personal information. The benefit for them is that they don't have to trick you into clicking on links or mentioning your personal information to an outside source: they get all of that information directly from you, without you ever knowing about it. There are ways to make this process more difficult for the cybercriminal and much safer for you, which we will also examine later in this book.

You can see how cybercriminals are focusing less on one, widespread method of getting into your systems, although these are still in use too. Often, however, they make specialized malware specifically for the platforms that you use and try to get you to interact with the infected links. Because of how well this malware blends in with the rest of the site, it can be difficult to traffic these social media platforms without accidentally interacting with a cybercriminal's attempt to get into your network.

The point isn't to frighten you off social media altogether, but to make sure you're using it in a smart, safe way so that your business doesn't get compromised while it uses all of these different social media platforms to its advantage. The key to doing that is to stay vigilant and knowledgeable so you can better differentiate between legitimate posts and cybercriminal activity, so that by identifying the threats, you can avoid them altogether.

The Consequences of a Social Media Cyberattack

So, let's assume that you take all the necessary precautions that you possibly can, but somehow your network still gets attacked and your information ends up compromised. How big is the problem, really?Unfortunately, it can be disastrous for your business.

If you don't protect yourself properly, you can wind up with a lot of your most sensitive information in the wrong hands. This could include your clients' personal data, your bank account information or other sensitive information about your business that you don't want getting out. Credit card fraud is especially common with these types of incidents, but you might also experience other consequences such as a shutdown of your account, activity on your accounts that you were not responsible for, or your systems being held hostage until you can pay the cybercriminal off (otherwise known as ransomware).

Obviously, any cyberattacks leveled against your business will hurt it in some way. Considering all the positive impacts that social media can have on your business, like garnering more customers or making their experience with your company more pleasant, you will be affected negatively by social media cyberattacks just by virtue of not being able to advertise or conduct yourself in the same easy way until the problem gets fixed or, if customer data has been compromised the damage to your reputation may be irreparable. Having to spend a lot of time, energy, and money rebuilding your reputation, or to purge your network of intruders, get your business back up and running cuts back on day-to-day operations and productivity too, which means less income coming in while you're dealing with the problem.

There are more pressing issues facing you as well: your funds could get stolen or your information could get released. While these consequences are naturally detrimental for any company, they're especially harmful to small business, companies that are just starting up and those that are undercapitalized at the time.

We'll get more into detail about these problems and how to solve them later in the book, but being aware of what could happen if you're not properly protected should act as the deterrent you need from being too reckless online.

What Cybercriminals Are Looking For

Cybercriminals don't just go after anybody that they see on the web. They're specifically looking for business owners that meet their needs who will be particularly susceptible to their underhanded tactics in one way or another. They're smart; they know what to look for and who to target. The best way to make sure that it's not you they go after is to understand what they want out of a profile and do everything you can, within reason, to make sure you're not doing those things.

The main thing that cybercriminals are going to look for is a lack of privacy settings and an openness about your personal and business information. If your passwords are your dog's name or the street you grew up on, and you're posting all of that information on your public personal profile, it's going to be much easier for a hacker to get into your accounts than if you made your passwords something obscure and didn't advertise them so openly.

It might be a good idea to change your passwords frequently to ensure that it's that much harder for an unauthorized party to get into your accounts. Using different passwords for your different accounts would also be a good strategy, so that if someone does hack into, say, your Twitter, they can't get into your Facebook, Snapchat, and all your other accounts too. Hackers will try to infiltrate all of your accounts to get the most information that they can on you, especially if your pages are all linked together. Keep them as separate and safe as possible without damaging your business's presence online.

Minimizing the potential damage should be your most important goal when thinking about how to combat potential cyberattacks before they happen. Knowing what cybercriminals look for in a potential victim and what attacks they like to keep in their arsenal could be what stops you and your business from being next.

Chapter FOUR

The Anatomy of a Cyber Attack

To give you a better understanding of what it could be like when your business becomes the target of a social media cyberattack, let's look more at instances of specific social media-based attacks that have really happened to companies. This should make it more real than talking about the possibility in the abstract.

The Mia Ash Case

Let's start with a recent account of a relatively big cyberattack that was uncovered just last year during July 2017.

This case study was executed as a series of attacks against several companies across MENA (the Middle East and North Africa), particularly in Saudi Arabia. A fake profile operating under the name Mia Ash would target businesses it deemed susceptible to cybercriminal activity. These attacks date from April 2016 all the way until July, over a year later.

The Mia Ash profiles operated first and foremost as a catfishing scheme. Catfishing is a term that's been gaining recognition since 2010. What happens is that a person or a group of people create a profile under a false name and with false pictures. This usually also involves elaborate backstories to uphold their fake identity and make it seem more credible. Catfish usually have multiple fake accounts to make themselves seem more legitimate, often posing as friends and family on top of the original profile. They're usually doing it to fulfill some sort of disreputable goal, like stealing your information or getting money from you.

Mia Ash would start by choosing a company to target and then reaching out to several different employees there. ‘She’ would then establish cordial relationships with them under the fake name and pictures. This was made easier by creating several Mia Ash accounts across multiple social media platforms, like WhatsApp and Facebook, making the profiles appear more legitimate and to further their reach.

‘She’ operated primarily on LinkedIn as her way of reaching out to members of a targeted business, and she would get these employees to accept her contact requests and slowly gain their trust. Once she had successfully done that, she began to engage in phishing schemes to get more private information about them and the companies they worked for.

Armed with this information, she could more easily start to go after the company itself, using the employee or employees as the entry point. Mia Ash would then use malware to get what she wanted. The fake profile specialized in trafficking a RAT, or a Remote Access Trojan, called PupyRAT. PupyRAT was delivered to the employee via email and, when that person inside the targeted organization clicked on the link from their company email account, it would open up a document that automatically downloaded the malware onto their computer. Just like that, Mia Ash was in the company network.

She was eventually caught by a team dedicated to finding major cybercriminals with help from organizations that had turned down her requests to talk. ‘She’ was uncovered to be a ‘they’: Mia Ash was being operated by a cyber threat group devoted to stealing this type of information from businesses for profit.

This case is a classic example of what not to do with your social media accounts and what can go drastically wrong if you put trust in the wrong people online.

The Mia Ash profile operated off multiple accounts, got people to divulge company information, coerced them into clicking on her malware-infected email, and took information directly from the company server. Just one person falling for a fake profile can lead to disastrous consequences for your business.

This case is also a good example of why you need to make sure that your new knowledge about social media scams is passed down throughout your entire organizations. Cybercriminals can and will target your employees and hurt your organization from the inside out. Make sure you're protected on every level of your business, from the top down to the entry-level worker.

The Uber Case

This was a different kind of cyberattack that should demonstrate why you need to be careful about how much of your personal information you're entrusting to social media platforms. This time it wasn't the individuals on the app who were targeted by a cyberattack, but the app itself—and that ended up leaving everyone who used the app vulnerable.

In late 2017, Uber came out with a startling confession: over a year prior, they had been victims of hacking. Hackers weren't targeting the business, though; they were going after all of the customers who used Uber instead.

These particular criminals had found out that Uber had stored all of their passwords and account information up on a software site. It was coded in their private account there. The hackers obtained that code, then used it to break into Uber's massive database and stole the names, emails, and phone numbers from millions of Uber users, as well as license numbers from 600,000 drivers. With this data, they then asked Uber for a ransom. They presented an ultimatum: Give them the money they wanted, or they would keep all this data and release it, putting all the victims at risk for being targeted by other cybercriminals.

That's pretty bad. Millions of people were put at risk after having their information stolen from an app that they had entrusted it to. But instead of letting the victims take the necessary measures to protect themselves from further damage, Uber decided to cover themselves instead. They chose not to mention that any of this had happened until November over a year later. This left the victimized customers in a bit of a panic, unsure if their information had been stolen a year ago and trying to make up for the lost time in protecting themselves if their stolen data had been used after all.

So what did Uber do instead of letting their customers know that they had been put at risk?

To make matters for themselves even worse, they paid the ransom that the hackers asked for to delete all the stolen information, in exchange for not saying that they had done this and keeping quiet about the whole thing. Effectively they were giving a free pass to cybercriminals everywhere to go after them again, potentially keeping and using the information they get out of it, since they're admitting that they will give the money and nobody will look for them or try to stop it. This is exactly why you should notify authorities instead of paying the ransom.

This whole mess ended up leading to a deep dip in Uber's customer pool. This attack combined with a host of other scandals was the final straw, and a lot of users called it quits and switched over to Lyft instead, which means a significant portion of their income just up and walked away. Just like that, Uber lost a portion of its customer base, tens of millions of dollars to one of its main competitors. Concluding that they haven't noticed any adverse effects from the incident and offering the victims remedies by way of credit monitoring and other protection wasn't enough to sway them back.

Now they're facing legal action and a serious investigation into their company for perceived negligence against their customers when they should have been protecting them. This case teaches you everything about what not to do in the event of a cyberattack: Don't wait to disclose a cyberattack, don't lie about it, and definitely don't pay off the hackers. It won't end well. As the saying goes, it's not the crime it's the cover up.

Although Uber isn't an app that would likely be linked to your business, this case demonstrates how other apps that you do use for your company, such as Instagram or Snapchat, can be targeted and leave you at risk. They're also a lesson on how social media cyberattacks can equal disaster for your business and a massive win for your competition.

The HAMMERTOSS Infection

Let's examine a particular form of malware now so that we can see how cybercriminals target businesses with a specific infection. It will be a good way to understand exactly how cybercriminals work. It will also be very helpful for you to understand how HAMMERTOSS works and spreads throughout your network, because it's been an active, operational piece of malware since 2015 and was still infecting networks as recently as last year.

HAMMERTOSS is malware designed by a highly skilled Russian threat group. It was first discovered by technology security experts in 2015. It works by using Twitter, GitHub, and cloud storage to get your data from your network. Let's focus on attacks originating on Twitter, because that is one of the main, very prominent social media platforms and one that you most likely have an account on.

It works like this: Cybercriminals would post commands on their own Twitter profiles. HAMMERTOSS would then automatically scan social networks, mostly Twitter, for such commands. Once it found an attacker's account, it would find the tweet with a URL and hashtag in it that had certain commands for the malware embedded and encrypted within the links. The infection would then find that information and just like that, it had its orders.

Once it knew what the attackers wanted it to do, this infection would visit random users' Twitter profiles every single day. Much like how real live cybercriminals monitor an individual profile for hints of information that it can accumulate into a pool of knowledge, HAMMERTOSS would similarly search for personal information on the account and compile that into a database of sorts. It would use knowledge it gained there of the targeted user's routine, particularly their work schedule, to communicate back to the attacker about the victim so that they would know when their target was at work and about other times and days when they were known to be away from their profiles. Compiling information on the victims in this way allowed the cybercriminals to more quickly and easily attack the specified victim and their company, while cutting down on the time and energy they spent monitoring the person themselves.

In a real-world example, HAMMERTOSS was used to find out when the CEO of ABC company (we're not exacerbating their problems by re-publishing their name here) had left for vacation and troll LinkedIn and other sites to find out their Executive Administrative Assistant. Once the hackers knew the CEO had left, they spoofed his email and had the assistant wire $500,000.00 to "hold the order at the current price." Because the CEO was unreachable at the time, she did as ordered and just like that the company lost $500,000.00

One reason the HAMMERTOSS infection is so important to study is that it helps you more effectively see the consequences of revealing all of your personal information on your social media accounts. Even if all of your posts containing sensitive information are spread out over a long period of time, HAMMERTOSS could still scan your profile and use old posts and combined the knowledge it gets there with more recent ones as part of its database of information on you.

As I discussed before, posting your location and activity every hour of the day could make you vulnerable to become a target of an infection like HAMMERTOSS.

Looking at these cases, you should get a better idea of what a cyberattack originating through social media looks like. Now that you can see where some other companies went wrong, hopefully you can use that information to arm yourself against similar attacks leveled against you and your business in the future. Remember: Protect yourself, protect your customers, and most importantly, protect your information.

Chapter FIVE

Protecting You and Your Business

Learning about all the different ways your social media accounts can become compromised might be making you start to worry right about now. If it can happen to big companies, who have the time and money to educate and arm themselves, then what's stopping cybercriminals from coming after your business next?

The answer is: You are.

There are several small ways that you can make your business profiles safer and stop cybercriminals from ever considering you for an attack. Now that you've seen how cybercriminals choose their victims and execute their plans, you should be starting to recognize the biggest pitfalls when it comes to your social media protection and understanding how you can avoid these same mistakes. There are also still some smaller ways that can help you achieve your goals of staying safe.

One of these ways is to be very careful where you are entering information, and what you have saved to automatically fill in. You shouldn't save your personal information online in case of clickjacking. You may think that you are just entering in your name and number, but if your address, credit card, and other important information is saved along with them, cybercriminals may be taking all of that information as well without you realizing it, even if that particular page isn't asking you for it.

Being aware of the biggest threats that cybercriminals level against small businesses is the best way to keep yourself guarded against their attacks. Here are some other small ways you can keep your business safe.

Maintain Password Safety

Be sure to have complex passwords for your social media to make them harder for anyone trying to get into them who shouldn't be. In the previous installment in this series, I go over in detail some of the ways you can make your passwords more secure. Just as an overview, you should make them difficult to guess by adding numbers, capitalizations, and different characters to whatever you choose. This will make it much harder for cybercriminals to get into your accounts and see personal account information that you don't want them seeing. Better yet, long phrases, which are easy to remember are the most difficult to crack because of their length.

For instance, My name is Al Alper, author and cybersecurity expert is nearly impossible to hack but very easy for me to remember, while A1A!per would still take long (approximately 1 month) it is much harder to remember where there was a number and where there was an exclamation point.

Be careful what you're posting for everyone to see as well, even on your personal account; your hometown, family members, pets' names, and any other personal information is very commonly used to make passwords, and cybercriminals know that. Posting this information everywhere makes your account unsecure.

You should try and avoid using anything like this in your passwords anyway so that they are much more difficult to guess, even if you don't post about it. Cybercriminals are looking for networks that are simpler to access, and you don't want to be easy prey. You should also use more than one password for all of your accounts to make it more difficult to get into your other social media if one of them is compromised. Don't give all of your passwords to one person, either; using a password manager or a similar tool ensures that you can eliminate human error and still grant access to any employee that you want.

Make sure that your passwords aren't written down anywhere, either on paper or on any device. This runs the risk of them all getting lost or stolen; neither would be good for your business, because somebody could steal it and because you might be locked out of your accounts until you get back those passwords, which could kill your productivity and put your business at risk. Leaving such information lying around, even if you think it is safely kept in the office, potentially gives visitors and even unauthorized employees access to it. You should be able to feel comfortable knowing that only those that you want accessing your accounts has the passwords to do so.

Avoid Posting Personal Information

Another good tip is to resist posting your location on all of your accounts, all of the time. Of course, it's unrealistic to never display where you are; often it can be good for business if customers are able to see where you are, especially if you're opening at a new location or having an expo for a day, or anything that you want as many people as possible to come to in a short amount of time. However, if your location is all over your accounts at every hour of the day, criminals will be able to track your movements throughout the week. They will start to learn your routine, including when you're in and out of the office, or away for an extended period of time. Like in the HAMMERTOSS example, you should never let people know when you're not around, because they will be able to tell when your devices are unmonitored or how to exploit your team through social engineering, and plan their cyberattacks accordingly.

Of course, no one can be in the office all day every day, and there are always times when your information and your network isn't under routine observation. These are the hours that cybercriminals are looking for. A good way to make sure that your network is still protected in these riskier hours is to get a person or a software service that can alert you if there is "suspicious activity" on your network, such as information being accessed at abnormal hours of the day or a user looking at files that they should not have access to. This is useful so that you or your systems administrator can be informed of this suspicious activity as quickly as possible and take the necessary steps to shut it down before your network is compromised and your business suffers. I will go into these services later on in this book.

Sharing Personal Information

Even on your personal account, being wary of when and with whom you're sharing personal information is critical. Many times, cybercriminals will target individuals in order to get at the network or business that they actually want to infiltrate and compromise. The biggest weak spot in your company, unfortunately, is you.

Cybercriminals know this. As a business owner, you want to advertise yourself in that position to give more exposure for your company, so that clients can put a face to the company and thus trust it more, and so that both employees and customers know who to turn to in times of crises. However, this widespread exposure is also what makes you vulnerable: cybercriminals know exactly who to target to try and get what they want.

For this reason, you need your personal account to be as secure as your professional one. You already know not to share too much openly. You also need to be careful of what you're sharing in private.

Don't share any deeply personal information with someone you don't know, even if you think you know them through the internet. As I mentioned before, catfish run rampant online, trying to gain your trust so that you'll send them money, share your passwords or bank information or other private knowledge, or—as with the Mia Ash case—just to garner enough little bits of information to eventually form a bigger picture and use that to go after your business. You may think you know someone, but you can never really know who is behind the screen. Only friend and share personal information with people you know and trust, even on your private accounts

Ensure Employee Discretion

We all hope that our employees have the business's best interests at heart, but they very likely won't care about security to the same extent that you do as the owner. For this reason, you should take steps to ensure that your employees are also being careful with information about your business. They should also be following the same steps that you are to protect passwords and maintain a balance of advertisement and discretion. Employees on all levels of your organization, from you all the way down to the new entrants, need to be made aware of how they should and should not be conducting themselves online, both at work and on their personal accounts.

This is a little trickier to do compared to following the steps toward security yourself. You can't personally teach everyone. A good way to approach this is to make sure that everyone is following the same security protocols and guidelines. Employee training sessions are a good method to educate them on the specific rules you want to implement in your organization while ensuring that everyone is on the same page about what the expectations are.

One of the things you might go over in these training sessions is how to be safe while on the network or on their business accounts. Educate them to the same extent that you now are. They should also be aware that they should not click on suspect links in emails or friend people that they don't know while on the company network or on their company accounts. Doing so may be giving hackers access to your systems, or at the very least they may begin mining the employees for information that, little by little, can eventually do your business harm, as is, again, what happened in the Mia Ash case that I discussed earlier on in this book.

They may also want to increase their privacy settings on their personal accounts. Leaving those pages open for anyone to see may eventually lead cybercriminals to sensitive information about your business. If an employee with low privacy settings lists your organization as their employer, makes posts about their daily life that reveal their or their coworkers' routines, and divulge seemingly inconsequential details about the business through pictures and other posts, they may be unintentionally leading cybercriminals to the one last key piece of information that will finally enable them to infiltrate your network.

Another component of safety that many employers have already implemented in some form or another is monitoring the way that employees talk about the company, or regulating what they say about it. Oftentimes, policies like these (whether formally conveyed or not) are meant to prevent employees from speaking badly about the company on their personal social media accounts, but you can also make rules about what company information you want employees revealing on their personal accounts, and what information is best kept private.

Of course, you can't demand that employees increase their privacy settings on their personal accounts or dictate exactly what they say online, but you can educate them during trainings so that safety, both personal and professional, is something that everyone is keeping in mind. Employees must be just as safe as you are while on the internet at work and at home, because the slightest slip-up could potentially turn into something a lot bigger, and a lot more dangerous.

Danger lurks everywhere, and cyber criminals rely on the fact that people will "check in" with their social media accounts during the workday. As leader, ensure you have an Acceptable Use policy in place is a great first start to reminding employees what they can and can't do on the business computers and network; including checking their own social media while on your business's network. One thing to keep in mind is that, as a business owner, you can't monitor every single employee at every hour of the day, especially as you begin to expand your organization. You probably want to. It may be tempting to completely ban the use of personal social media accounts on the company network, but people are likely going to be checking their Facebook feeds in the break room and updating their Twitter about their day.

A ban on employees' personal social media may slightly suppress the amount of people going on their accounts on the company network and company time, but it will only encourage others to be more discreet with their usage and, worse still may begin to foster unrest and or unhappiness in your team. Thus, employees are much more likely to follow regulations about their personal social media use than they are to entertain a complete ban on it.

Cybercriminals are aware that it will be most effective for them to use every level of an organization when trying to break into that business's private network. They can, and will, use a combination of your business accounts, your personal social media profiles, and those of your employees as well, to socially engineer a profile on your business and increase their chances of getting inside.
Think of it this way: Even if every employee only put a single private detail about the business onto their personal social media accounts, the effect of all of these pieces of information combined could be very damaging for your organization. Everyone's account needs to be secure, or nobody's account will be.

Try to incorporate all or at least some of these strategies into your everyday work routine. Don't dwell. Otherwise it can become all you think about, and if it gets too overwhelming, you may not want to do it at all. By including these smaller safety tips in your routine, it can become easy and effortless to protect your business.

Chapter SIX

Ensuring Long-Term Protection

Although everyday steps to protect your business is necessary, you should also take overarching measures to shift how you view protection. By making some bigger changes in your methods of network safety, you can help ensure the security of your business in the long run at every level of your organization.

Here are some of the biggest ways you can ensure that your business stays safe on by shifting your behavior and attitude toward security.

Monitor Your Transactions

The advice from the previous chapter about monitoring unusual activity on your network can go for more than just strange system activity, too. As businesses move further into the cyber sphere, transactions are becoming more digitized as well, and that's something to watch out for.

Make sure that you are getting notifications about any transactions into or out of your bank account as soon as they occur. Whether you are moving money directly through the bank, using a third party service like Paypal, or making deals through apps like Venmo, turn on instant notifications so that you receive a text message, call, or other alert when any unordinary activity occurs. Should something happen, you will be able to more efficiently report it and deal with the problem instantly. You'll be notified for any real transactions made by doing this as well, so you can verify as you go that they are legitimate.

Some services that are linked directly to your bank account or credit card, like Venmo, lets you add a PIN to your accouLLint that you must type in before payments go through. This will ensure that any fraud that might occur only affects your Venmo balance, and not your actual bank account, and is thus much easier to rectify. Whenever you can, take whatever steps you can to distance apps like this from automatically making transactions. Always leave room for human error and for cybercriminal threats and activity.

With Venmo, you might want to also consider linking your account to your credit card instead of directly to your bank. It may cost a bit more, but it won't automatically drain money from your account when a transaction is made, thus making it easier to deal with any issues that might arise before you have to pay—literally.

Also, consider keeping your transaction information private instead of publishing it to the feed, for the same reason that you shouldn't post all your personal information and day-to-day business on other social media platforms.

Anything you can do to keep stalkers from seeing your business, particularly with something as dangerous as your financial history, can only help you in the long run, even if it doesn't seem like a big deal now.

You should also leave some money in your balance so that you aren't pulling the money directly from your bank account or card every time. Sometimes scammers will appear to pay you, but if they are using a stolen credit card or if they dispute the charges later, Venmo can take back the money, even if several days have passed since the transaction. Once it enters your bank account, it's YOUR responsibility and thus much more difficult to get back. Apps like this may be fast and easy to use, but they don't guarantee payment the way other sites, like Paypal, do. Try to maintain as many degrees of separation from your actual bank account as you can.

Whatever happens, make sure that you are reporting problems such as spam, abuse, or fraud as they occur. Most websites have a feature that will allow you to flag suspicious users, ads, and posts. Not only will this protect yourself, but it will help future users stay safe as well.

Monitor Your Network

I mentioned in the previous chapter that there are certain services that will alert you whenever any suspicious activity is detected on your network. Services like these are possibly the best way to know whether or not your accounts are being accessed without permission; social media activity in the middle of the night is probably coming from someone outside of your organization, or at least from someone other than the specific employees who are meant to be running those accounts. The same goes for any activity during hours that you know nobody should be in the office.

Although almost every social media platform out there will inform you what time of day they were updated, so you should be able to tell by checking the time stamp whether or not a post came during a suspicious hour of the day, monitoring it yourself will not allow for optimal efficiency. You may still not notice for hours that suspicious activity has been detected. You also won't notice that anything is wrong if the account was simply accessed. As long as the intruder doesn't post while they're trespassing, there will be no trace if you're just checking the feed.

Let's face it, it's impossible to catch everything. However, monitoring software will allow you to tell as its happening that Let's face it, it's impossible to catch everything. However, monitoring software will allow you to tell as its happening that someone is on your account when they shouldn't be, whether or not they post any updates or change any account information.

Here's where hiring a technology expert could come in handy. Running your business, you probably don't have the time to be constantly on alert for cybercriminals and breaches in your security. Contracting or hiring cybersecurity company or person with the time, resources, and skill to be in charge of your protection will give you more time to focus on running your business.

Manage Your Social Media

Although you may have a firm grasp on what will compromise your business and how to avoid it, the fact is that you are not the only one making day-to-day decisions about your social media. As your business expands, you might begin to hire others to whom you delegate the task of maintaining your social media presence, and they have to be equally trained in how to prevent cybercriminals from gaining too much information and access to your accounts.

You should want to have more than one person managing all of your organization's social media accounts. Having one person with all of the knowledge is inherently dangerous, especially if something happens unexpectedly such as they fall ill or quit and you are left without access to your accounts for a period of time. Also, if only one person is in charge of all of your accounts across every single platform, there is an increased likelihood that they are all linked together; Facebook might be used to log into Instagram, which could connect to your Twitter, etc. If one linked account gets hacked into, then all of the other accounts are susceptible too. This is especially true if personal accounts are linked to professional ones, because then the information on those personal accounts can be used to get into the professional accounts. Of course, sometimes linking accounts is necessary, as it is for LinkedIn; unless you have to, though, you should try to keep them all separate. Having different people in charge of each one is one way to guarantee this.

Maybe you're worried that there will be a disconnect in the "voice" of the different accounts, or that information will get lost in translation between the people in charge of them. One easy way to spread the responsibility and still ensure that there is consistency is to have a main administrator in charge with several people working underneath them. They should be trained and experienced in running successful social media accounts, aware of how to maintain protection on those accounts, and good at garnering business and attention through the use of these platforms at all. By putting someone knowledgeable at the head of the team and having several people reporting to them, one person is still "managing" all of your social media, but protection is much better maintained.

There are applications that will manage all of your social media accounts as well. They are a terrific time saver, but beware. They are susceptible to hacking, so use care in password complexity if you go this route. Where possible, use multi-factor authentication for these types of applications and all of your accounts.We'll talk more about this later in the book.

Stay Up to Date on Privacy Settings

Social media platforms are constantly changing and updating, often with the goal to connect you to more people on their site. Social media platforms are, first and foremost, business ventures in and of themselves, and as such the developers are looking out for their own self-interest when making any updates or changes. Since it isn't always about doing what's best for their users, these updates aren't always good for your business and it isn't always what you want in terms of privacy.

For example, two recent updates that some social media websites have implemented is location detection and facial recognition. Automatically, location services are turned on for certain platforms like Snapchat, and you have to manually turn it off if you don't want people who follow you there to be able to see exactly where you are at all times. Facebook just launched a new update that will detect your face in pictures that you aren't tagged in.

Several platforms also have what is known as "geotagging," which is where they automatically list the location of where you made a post as you make it. In some instances, like on Snapchat and Instagram, this is public and obvious; you can geotag your own pictures if you choose. Other platforms have invisible geotags that hackers can find if you aren't careful and turn off location services for those apps, because you won't even know that that information is embedded in the pictures.

All these things have the potential to connect your business to outside locations that you don't want or need to be associated with. You should always keep up to date on emerging updates so that you can adjust your settings accordingly, whether you want to utilize these updates or not.

In contrast, many platforms are updating their settings and making your accounts more secure when they do. You will want to be aware of these changes as well, particularly because not all of these updates will automatically take effect just because the website updated. You often have to turn these changes on in settings to get them.

There are applications that will manage all of your social media accounts as well. They are a terrific time saver, but beware. They are susceptible to hacking, so use care in password complexity if you go this route. Where possible, use multi-factor authentication for these types of applications and all of your accounts.We'll talk more about this later in the book.

Stay Up to Date on Privacy Settings

Social media platforms are constantly changing and updating, often with the goal to connect you to more people on their site. Social media platforms are, first and foremost, business ventures in and of themselves, and as such the developers are looking out for their own self-interest when making any updates or changes. Since it isn't always about doing what's best for their users, these updates aren't always good for your business and it isn't always what you want in terms of privacy.

For example, two recent updates that some social media websites have implemented is location detection and facial recognition. Automatically, location services are turned on for certain platforms like Snapchat, and you have to manually turn it off if you don't want people who follow you there to be able to see exactly where you are at all times. Facebook just launched a new update that will detect your face in pictures that you aren't tagged in.

Several platforms also have what is known as "geotagging," which is where they automatically list the location of where you made a post as you make it. In some instances, like on Snapchat and Instagram, this is public and obvious; you can geotag your own pictures if you choose. Other platforms have invisible geotags that hackers can find if you aren't careful and turn off location services for those apps, because you won't even know that that information is embedded in the pictures.

All these things have the potential to connect your business to outside locations that you don't want or need to be associated with. You should always keep up to date on emerging updates so that you can adjust your settings accordingly, whether you want to utilize these updates or not.

In contrast, many platforms are updating their settings and making your accounts more secure when they do. You will want to be aware of these changes as well, particularly because not all of these updates will automatically take effect just because the website updated. You often have to turn these changes on in settings to get them.

If, for example, a platform that you use launches an update that allows you to add a PIN to your account that must be entered before purchases can be made, or that will shield your email and linked account names that you have associated with that one specific platform, you may or may not want to take advantage of that. Maybe you even want to turn on location services so that potential clients can always know where to find you. Depending on your business, there are certain updates that you'll want to take advantage of and others that you should definitely avoid. Only you can make that call.

No matter if you want to turn these services and settings on or off, you have to be aware of them before you can make that decision. Update your platforms when new versions come out. Read about the changes that have been implemented, then decide accordingly whether or not that's something you want for your own page. Research, knowledge, and conscious decision-making is the only way to make sure that you are managing your accounts' privacy settings the way that you want them done.

Layered Security

Everything we talk about above are terrific steps to take to protect your privacy and secure your social media profile; they do a long way at protecting you online. But along with these steps, it is important to mention other security measure you can and should take to protect yourself online.

Access to social media begins with a username and password. While we've demonstrated that people, by their own hand give hackers all of the information they need to know your username and crack your password, there are additional tools you can use to further secure them. We call this layering.

With layering, after you enter a username and password, the system will require another authentication method that is only available to you to verify who you are before you can access your account. Most commonly this is multi-factor authentication.

Built right into most social media platforms is multi-factor or two-factor authentication (MFA or 2FA). MFA is a method of verifying that you are the person who is entering your credentials (username and password). This is done using another device like your cell phone, smart phone or email account to verify who you are. We'll use Facebook as an example.

When you setup your account, you have to provide Facebook with a valid email address to verify your account. In addition, you can give them a cell number to use. Facebook's MFA will use your email or cell phone for MFA if you have it turned on

see https://www.facebook.com/help/148233965247823

Once you enter your username and password to login to Facebook, it will send a text message to your phone with a code. You will have to enter that code on the next screen before Facebook will allow you into your account. Because you have the phone, hackers won't have and can't get the code. Similarly, if you choose to use your email, a code will be emailed to you to use and enter.

Layering security a terrific way to limit access to your account and keep cyber criminals out. Most platforms, whether they be social media or social media management platforms or even your own office applications support some form of layered security.

Moreover, layered security can and should be used to protect your company's network and systems. Firewalls, antivirus and antimalware, password complexity and rotation policies, spam filtering, DNS and web protections, backup and disaster recovery appliances and software, encryption; these are all terrific solutions that protect components of your system and private information on your network. When used in combination with one another they create a robust, layered protection for systems and network.

Chapter SEVEN

Current and Incoming Security Measures

Cybercriminals are always evolving when it comes to ways to get into your private networks. The flipside of this, however, is that security and protection is always evolving as well to combat these threats. You're not the only one fighting to save your business, and there are many different laws, programs, appliances, and software out there designed to help you keep your business safe.

In this chapter I'll go over all the things that already exist for your protection, as well as the new legislation and software coming out soon for your use.

Current Network Protections

I have already discussed some of the things that already exist that are designed to help you out, such as hiring someone or installing something to monitor your business's network activity and notify you if somebody has gained access to information that they should not be cleared to view, or if there is activity at odd hours of the day or night when nobody should be online. There are plenty of companies that offer this type of monitoring protection, and doing some quick research to find out which network activity monitoring system is the best fit for you that also falls in your particular price range can save you a lot of time, energy, and money in the long run if an attack does occur in the future.

This same advice can be applied when trying to find someone to monitor your network security for you. Be sure to look for someone or a company that specializes in cybersecurity. Many IT service firms and individuals, while good at IT aren't up to date on the current threat landscape or specific technologies available to harden the attack surface. To them, a firewall and antivirus software are considered protection, but to a cybersecurity company they are the beginning of protecting you hardening the attack surface. Like a heart surgeon is to a general practitioner, a cybersecurity company or person is to an IT company or person. Specialization is key if you want real security.

Other ways to keep your information safe is to potentially join or review one of the many information networks available for sharing knowledge about cyber threats as they arise. These platforms are designed to let you know about growing, changing, or emerging cybercriminal activity as they're discovered, giving you the most up-to-date information about cyber-attacks, cyber threats and cybercriminal activity that's out there.

Examples of platforms like these include Mitre, which is a government-funded research and development website where they publish archives of all different types of cyberattacks so you can easily see what the most popular threats are at any given time. Other sites, like Sophos' Naked Security and ZD Net's Zero Day provide well researched information on the current threat landscape and solutions for threat mitigation, while sites like Microsoft Interflow and Cyber Observables as well as other information exchange websites, let users share information and knowledge about cyber threats with each other. It's a sort of social media for exchanging information. What these sites do, essentially, is help keep you aware of the current popular cyberattacks out there by connecting you to other users who can give you up-to-date information about threats that predominately affect small businesses like yours and operate across social media platforms.

In addition to network monitoring and exchanging information with others like you, there are certain laws already in place meant to protect you and your business from cyberattacks.
Should you choose not to involve the police when you experience an attack, you should first know that contacting law enforcement will give you the best chance of recovering any stolen data, money, or information. Moreover, if you plan to put in an insurance claim to cover your costs of recovery, they'll require that you contact the authorities.

Regardless of if you choose to go down this route, however, know that you should avoid using the compromised platform or network to communicate with other areas of your organization about the attack; the cybercriminal could already have access to more than the obviously infiltrated area of your network, and using your own system to alert the rest of your company to the threat could potentially be alerting the cybercriminal, too, and it's harder to take them down when they know everything that you have on them.

Should you choose to go to the police, you should know the law surrounding what you're experiencing. Certain acts are strictly prohibited by current U.S. law with regard to what others may or may not do online. Should a cybercriminal somehow gain access to your social media account, it is explicitly illegal for them to publish or use anything that you have a copyright on; whether or not they were aware of committing copyright infringement, they're still in the wrong. It is also illegal to commit fraud or tamper with any of your online communication, and to commit identity theft. Hacking and unauthorized computer access is also highly illegal regardless of context, as is eavesdropping on private communications with the intent to use any gained information in a crime.

More recently, the federal government passed a law in 2016 called the “Prevention of Electronic Crime Act” meant to give further funding and power to cybercriminal law enforcement. In early November 2017, a law was passed called the “Strengthening State and Local Cyber Crime Fighting Act of 2017.” This law will require that people in the judicial system get further and more in-depth education on current cyber-related threats and the proper investigations of such crimes. This law will, overall, ensure that cybercrimes are reacted to and put on trial much more swiftly.

There are plenty of laws already in place meant to protect you and the information that could be gained from unauthorized access to your social media accounts. Often, proving guilt can be difficult with online crime. However, knowing what is and is not illegal with regard to information that could be gleaned from your social media will help you better understand how to protect your accounts. Knowledge, as they say, is power.

Security Legislation in the Pipeline

Now that you know more about the laws currently in place to protect your business online, you should also be aware of what upcoming legislation is being implemented so that you can stay up-to-date in your protection attempts as time progresses.

There are currently attempts to shrink the scope of PECA, the 2016 law mentioned in the last section, due to a fear of its infringement on an individuals’ freedom online. The repeal or amendment to that law could leave your business open to more attacks. However, since most cybercrime regulations in the United States are determined by the states, there is some opportunity to learn by example: the E.U. recently passed the General Data Protection Regulation, which heavily increases fines for data breaches within the country, and which will go into effect in May 2018. Depending on how that works out, some states might look to follow their lead.

Furthermore, there is an attempt now to strengthen defenses against cybercriminals on an international level by imposing worldwide laws against cyber-attacks, instead of leaving it up to individual domestic governments. However, this has been highly contested in the past and will likely not be passed on a large scale anytime soon.

Laws always change as we see how effective or not they are, and we can begin to see whether or not they truly impact the level of cybercrime going on. We learn and change the laws or parts of the laws accordingly. As time progresses we will begin to see more effective legislation getting passed and amended. Cyber space will only continue to get safer.

Incoming Software Protections

Similarly to the way legislation gets changed and added as we learn more about what most effectively stops cybercriminals from breaching our accounts, so too does technology advance. Even now, the network monitoring software that I've already mentioned is being constantly improved. Current trends in AI (artificial intelligence) and software learning inform the programs as you and your team use their machines and traffic the network. The programs begin to "understand" what a normal state is then will alert when that states changes to abnormal. They are effectively learning, adapting to your behaviors and are better able to protect your network as well. The technology that is coming out that will be able to more efficiently learn your routines and behavior so that it knows when to alert you or flag something as suspicious activity. This will only increase the safety of your business's profiles and accounts.

Along this same vein, cybersecurity experts are developing more effective automatic security protocols that will allow your protection software to oversee and deal with routine security operations on your network, which will let those same security experts responding to deviations in your normal network activity to set up more effective combative measures, better prepare themselves and your network for bigger and more serious cyberattacks, and spend more time and energy dealing with the less routine challenges to your security.

Another emerging technology is one designed to use blockchain as a method of fighting cybercrime activity. Blockchain is a list of records permanently stored in cyberspace, where each “block” of data connects to a specific timestamp and information about any transactions between two parties. Most famously, blockchains are known for monitoring bitcoin transactions, but they are also applicable to any form of cryptocurrency being exchanged.

More recently, developers and innovators have been working to expand the scope of blockchains to do more than just record data; they want to enable them to assist with matters of cybersecurity as well. Using the links and blocks of data that blockchains already possess, some experts are working on offering users a chance to work on new operational platforms based on blockchains, where you can “rent” your extra bandwidth out for further cybersecurity measures that would protect you and all the other users on the platform against certain attacks, like denial-of-service attacks. This would take a lot of the responsibility on you, the small business owner, and put it onto the server itself. It would also fundamentally make any online interaction you do on social media much safer because of the built-in cybersecurity of these platforms.

Always keep an eye out for emerging software protections. As cyberattacks evolve and adapt, cybersecurity rises to meet each new challenge. You'll want to stay ahead of the curve.

Protective Hardware Devices

As security software improves to meet your needs, hardware devices will also evolve to help you in the near future. One of the most important things you can do is make sure that you have the strongest and most up-to-date protections available to you. Having powerful firewalls and anti-virus protections is one of the simplest and best ways to ensure that you are as protected against potential threats as you can be while still going about your daily business online.

Make sure you have a system of backing up your data and information outside of your network, as well. As we've seen, many cybercriminals will encrypt or steal files during a breach so that you can no longer access them; having a secure compilation of this information outside of the network, and therefore outside of their reach, will ensure that you are not left vulnerable in the event that something like this does happen to you. Invest either in the Cloud or a physical device that will let you access your files apart from your network.

Chapter EIGHT

Technical Terms Explained in Plain English

Backdoor access *– when hackers find unprotected parts of your server and get in through an undocumented gap in the administrative portal*

Blockchain *– a system that records the transactions of cryptocurrency between two parties*

Catfishing *– a social media scam where someone creates a fake profile to trap others into giving them money, information, or to fulfill some other goal or purpose*

Clickjacking *– type of hacking where the cyber-criminal layers an invisible webpage over the one that want to use so they can record the information that you enter*

Cryptocurrency *– any type of digital currency where the units and transfer of it are regulated by encoding it so only you and the other party can access the transaction information*

Distributed Denial-of-service (DDOS) *– type of hacking where the cyber-criminal finds a way to deny administrative access to you and anyone else with that level of clearance, either temporarily or permanently.*

Geotagging – *when a post on a social media site assigns and displays the location of where it was posted, either embedded in the post or openly displayed along with it*

Malware – *any software installed with the intention of damaging your computer, your files, or your network system*

Phishing – *a type of hacking where the cyber-criminal steals private information by tricking you or somebody else into giving it up, usually through spam or some type of theft of your account information*

Ransomware – *a type of malware that forces victims to pay a fee online to get access to their systems or in order to reacquire their stolen data*

Remote Access Trojan (RAT) – *a type of malware that lets cybercriminals take control of your system from a remote network*