Safe Computing Best Practices for End-Users: What You Need to Know to Keep Yourself Secure!

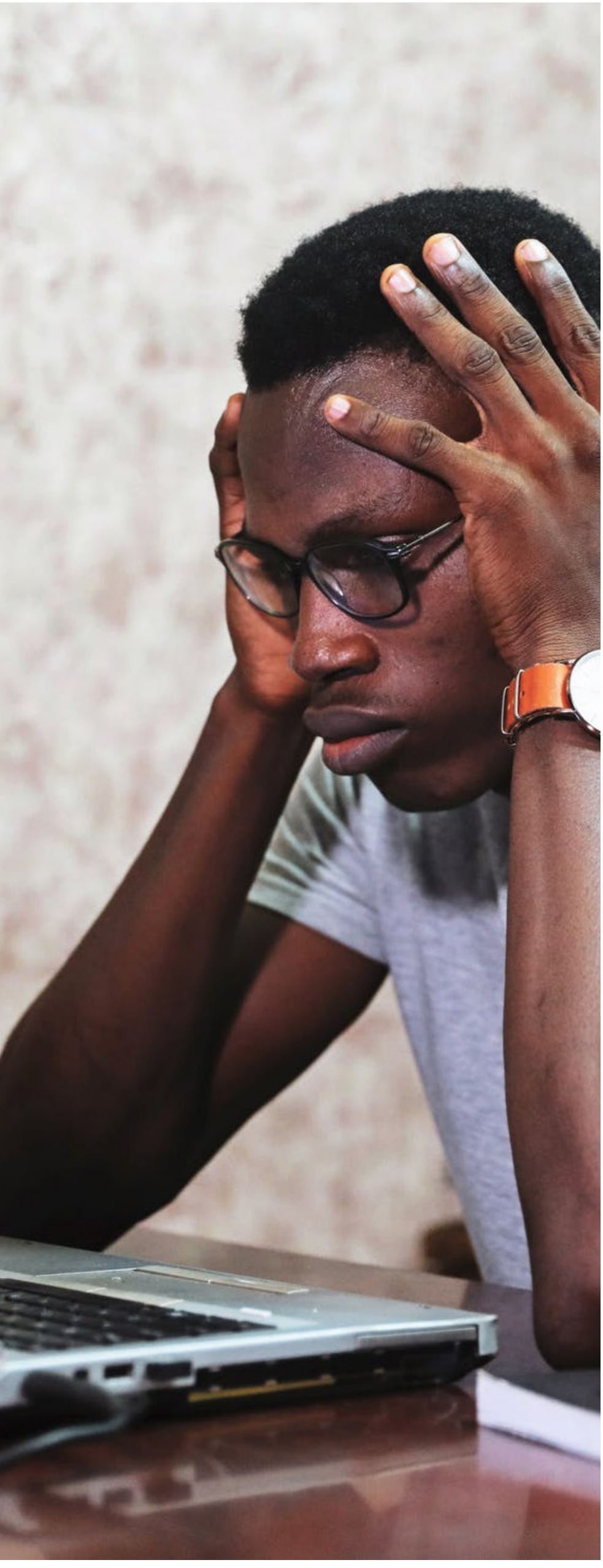
Imagine, back to the first few days of your job. You were, no doubt, eager to get started and eager to prove yourself. You would have been given new technology to work with; a laptop, a phone, maybe a tablet. You would have also met new people; your team, your boss, maybe even some of the executives you'd indirectly be working for. You may have felt hopeful as you embarked on this new journey.

On your fifth day of work, you get an email from a member of your executive team, asking you to buy two $500 gift cards.

Seeing that email, you're confused. Surely you're not the right person for this? You've just started at the company, But, if they're an executive from your organization, you certainly don't want to disappoint them. And, if it's really urgent, you'd better do what they're asking – fast!

So, after a few more minutes of indecision, you head out to purchase the requested gift cards. When you return to the office, the email from the executive requests that you scratch the back of the card to reveal the activation codes, then send a picture of both the front and the back of the card.

You send the picture as requested then, you wait. You don't hear from the executive for the rest of the day, but since they're in meetings, you're not really expecting a response. Still, a "thank you" would have been nice.



This early in the game, you're not really sure how to submit an expense claim to get reimbursed for the money you spent, but you have made a friend in HR – the coordinator that's been so helpful to you for the past few days. So, with receipt in tow, you head to their office to ask them how to submit the $1,000 claim.

After you explain the situation, you're concerned to see that their face has gone a little pale. The HR representative then tells you that the email you received was not, in fact, from the executive you thought it was – you've been the victim of a phishing attack, and you've fallen for it… hook, line, and sinker.

Think of the emotional toll this would take on someone… shock, fear, dismay. The thoughts swirling around in their head would be numerous. How is this going to impact my new job? How did I fall for this scam? What do I do now? Is my boss going to think less of me? How am I going to get my money back?

There is nothing worse than feeling like a victim; whether you're new at a company or a 15-year veteran. That's why we believe that, in this day and age, everyone should be aware of how important cybersecurity is, and how to recognize when something seems… off.

Table of Content

Chapter 1:

9 Phishing Attacks
11 Why Does Phishing Work?
13 Spear Phishing plays on Human Emotions

Chapter 2:

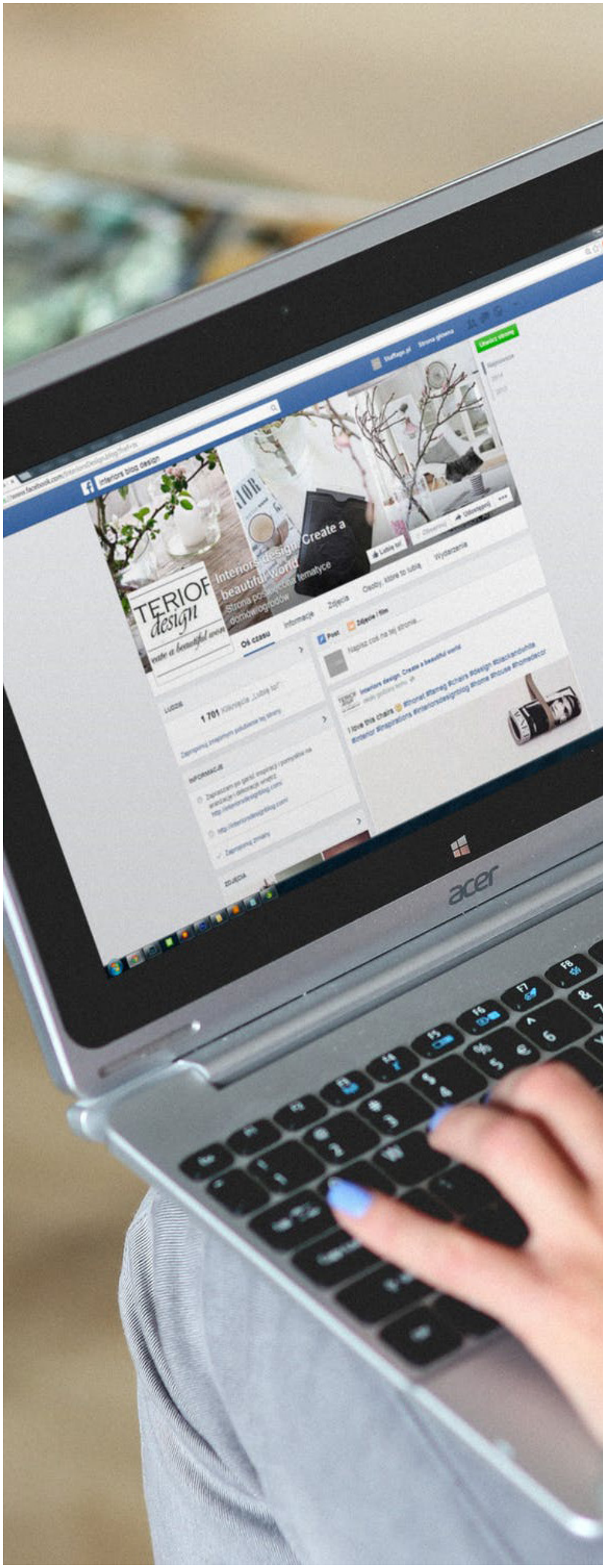
15 Social Engineering & How Social Media Plays a Role
16 What is Social Engineering?
17 The Four Phases of Social Engineering
18 How does Social Media Play a Role?
20 Beware the "Fun" Games You See
22 How to Protect Yourself Against Social Engineers

Chapter 3:

24 Password Management
25 Password Management Best Practices
26 Five Ways to Secure Your Digital Life With Regard to Password Management

Chapter 4:

29 Putting It All Together



Everyone is a Target!

Whether it's for monetary gain, or to gain access to sensitive information, or to cripple an organization that they disagree with, threat actors (hackers, to some) are out there, and they're actively trying to worm their way into your life and, more important, your IT infrastructure. This infiltration can be accomplished through sweet-talking someone into giving them access, forcing their way in through unsecured vulnerabilities that you may not be aware of, tricking someone in your organization into revealing sensitive information like usernames or passwords, or (to put it bluntly) kicking in your 'front door' with a brute force attack.

It doesn't matter how big or small your organization is, nor does it matter what industry you're in – any and all data is valuable to these threat actors, and they'll stop at nothing to get it. As an end-user, you may not always think about the security of your organization as falling under your purview – maybe you have an IT department that handles it for you, or you don't think you're important enough to be targeted. But, the reality is, most of us don't have a clue how our daily computer habits or behaviours can attract threat actors and make your organization a juicy target.

You are the First Line of Defense.

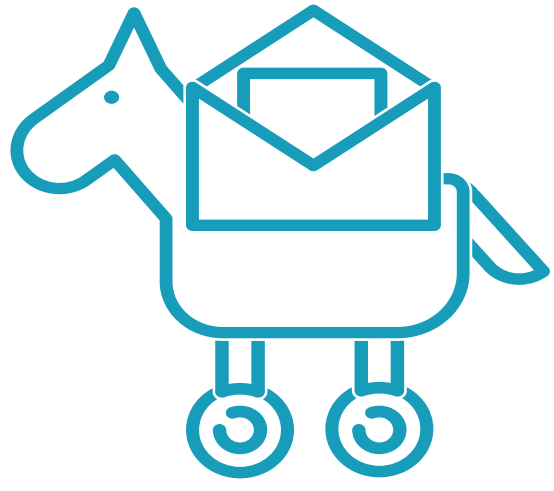
Like the new employee in our cautionary introduction, end-users need to understand the importance of cybersecurity from an end-user perspective. Can you recognize a phishing attack when it's happening to you? Are you aware of, or have you ever received training on what new threats are out there? Does your organization share information about what to watch out for?

The truth is, many organizations out there don't really have a basic security plan in place, nor are they training their end-users, like you, on how to identify and handle potential security threats.

And yet, it's the end-users, like you, who are the first line of defense for your company. You are, arguably, one of the most effective tools that your organization has in order to keep itself safe from cybersecurity attacks. The company that doesn't educate their end-users is like a person who is trying to keep a flood at bay using a screen door – it's not going to work!

This eBook has tips for you, the
end-user, explained in plain English.

Everything in this book has been
written with you, the end-user,
in mind.



Chapter 1:
Phishing Attacks

You've probably seen an email like this in your inbox at least once or twice over the years:

A solicitor or financial consultant from a European country emails you to say that his/her client invested 15 million of their currency with him/her, and they're now deceased. If you help the solicitor, they'll give you a percentage of the money.

A senator/lawyer/government official from Nigeria claims they've found a file at the Central Bank of Nigeria with your name on it, and they're trying to make sure you can receive your payment. They provide you with reference numbers and ask for your personal information for identification purposes. They tell you to act immediately so that you don't lose the money in the file.

Someone contacts you to say they've been in an accident or they've contracted a serious, debilitating illness, but they believe that you're trustworthy enough to be the business manager of their large sum of money (typically in the millions of dollars), and tells you that if you help them, they'll pay you a percentage of their money. They ask for personal information to get in touch with you.

These are phishing attacks, which are, surprisingly, still effective to this day. But the question is, why are phishing attacks so successful, and why are threat actors still using them? What are the threat actors looking to learn when they phish individuals or companies?

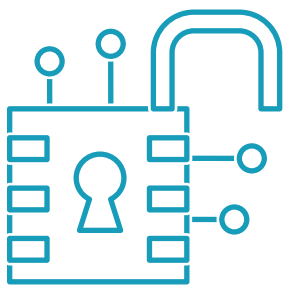
In our experience, phishing is typically done for these four main reasons:

Straightforward monetary gain.

Take, for instance, our new employee scenario. With just a single email, the threat actor in the example was able to trick someone into giving them a thousand dollars in Google Play or Visa gift cards. When you consider that they probably obtained the email address off the Dark Web for a few dollars, that's a pretty good return on investment, from the hacker's perspective.

Gathering account information about you, or others in your organization.

Sometimes the threat actors are using their phishing attacks to gather account information about you or others in your organization. If you hold a more senior position in the company, the hacker may be interested in phishing you so that they can use your credentials to impersonate you and cause further harm or gull unsuspecting employees, like our new employee scenario, into doing what they ask.

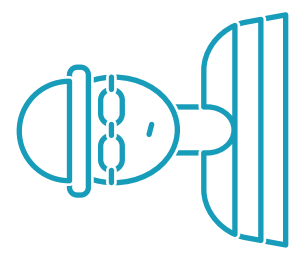


Hijacking your computer or entering your IT network.

Nefarious threat actors also use phishing attacks to trick you into entering your account information, like your username and password, so they can either hijack your computer or access your IT network. What's even worse is that sometimes, they're not looking to do something immediate. Sometimes referred to as a "sit and wait" approach, these threat actors may use your credentials so they can sit in your network and gather intelligence on what your organization is doing before they use that information to their advantage.

Installing malware on your device, or in your network.

Phishing attacks can also be used as the delivery method for various malware threats, such as ransomware, viruses, spyware, and others. The hacker does whatever necessary to trick you to click on their link, which then installs malware on your device for whatever nefarious reason they have (and this could be anything from stealing your data to completely shutting down your IT network).



Why Does Phishing Work?

Simply put, phishing works because we (the recipients) are human, and hackers are playing up to our human emotions and our human nature. Think of some of the most common phishing scams you may have heard of:

- Banks.
- Amazon.
- The Canada Revenue Agency or the Internal Revenue Service.
- Netflix.
- Your boss.
- Your company's CEO.

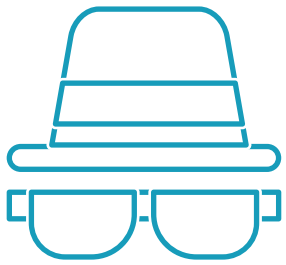
Phishing attacks these days are getting more and more believable. And all of these scams mentioned have the human factor going for them.

They're from people or companies who are familiar to the victim, so thevictim is more likely to trust that it's a verified request.

The message is often urgent, demanding that the victim "act now or else…".

And, contextually, it makes sense! Who really questions an email from their boss or the CEO of their company?

Hackers need to be persuasive, and they need to ensure that you don't question what they're asking you to do.



So, they've turned to far more sophisticated messaging that's designed to play into your immediate fears or innate desire to be helpful.

- My bank is emailing me and they're going to suspend my account if I don't do something now!
- The CRA or IRS has a warrant out for my arrest!
- Amazon's going to shut down my account if I don't verify it!
- Netflix needs my credit card information or they're going to send my account to debt collectors!
- My boss (or my CEO) needs something from me and I want to make a good impression on them!
- My HR department just emailed me to say I'm being laid off!

When you think about it, who wouldn't respond to an email or a message with this kind of tone?

This is what threat actors are betting on.

Spear Phishing Plays on Humman Emotions.

Spear phishing is the single most common (and most effective) social engineering tactic out there. We've touched on it a bit in the previous section, but spear phishing happens when a threat actor uses email to masquerade as someone that you know and trust, in a targeted email attack against you.

In a spear phishing attack, it's common for the threat actor to impersonate someone that you wouldn't normally question. Your CEO. Your HR department. Your IT team. A customer that you've worked with. An employee or co-worker who needs your help.

The new employee scenario that we talk about in the introduction to this eBook is an example of spear phishing that actually happened to one of our summer interns. Eager to do as the CEO asked, and new enough not to realize that our CEO would never ask for an employee to purchase gift cards, this intern fell for the spear phishing email that was, it later turned out, sent to several employees in our organization.

This is not the only time ProServeIT's been a target of spear phishing. In fact, one of ProServeIT's longtime employees found themselves without a paycheque for a few weeks because someone claiming to be him emailed our accounting department and authorized them to change the bank account number on file to another banking institution.

This incident led us to change our policies on how we accept such requests to verify that the person asking for the request is, in fact, who they say they are.

The point is, spear phishing, like other phishing attempts, plays on human emotions. They rely on something called Social Engineering, which you may have heard of. In our next chapter, we're going to dive a little deeper into it, so keep reading!

Chapter 2:
Social Engineering & How Social Media Plays a Role

Imagine that you get a phone call one day. When you pick up the phone, the voice on the other end of the line says, "Hello, this is Dave from your IT department, and I've just received a notice that you have some unusual activity on your account. Looks like you picked up a virus – we think we've caught it before we lost any company data, but in order to remove it from your machine, I'll need to sign into your account to take care of it. I know your email address is johnsmith@abccompany.com... I'll just need your password and we can get this cleared up right away."

What would you do? If you're in a larger organization, you may not even question this caller. How would it be possible for you to know everyone in your IT department? If the caller is claiming to be from your IT department, and they've got some preliminary information on you that they use to "verify" they are who they say they are, what's to stop you from handing over your email and password?

This is what Social Engineers count on. They're looking for ways to con you into an emotional, gut reaction, rather than rationally thinking things through and asking the questions you should be asking. In this particular instance, they've got you focusing on the fear of picking up a virus that may compromise company data.

The hacker's using all the right buzz words to elicit fear and compel action (fix it now!).

What is Social Engineering?

Social Engineering is the use of deception to manipulate individuals into divulging confidential or personal information that may be used for fraudulent purposes. They use psychological manipulation and often focus on various human emotions and human traits to trick people into giving out that personal information.

Phishing and spear phishing fall into this description, however, they aren't the only kinds of social engineering out there. In fact, social engineering doesn't even need to be done via a computer! The IT example we talked about was done via phone (what some in the industry are calling "vishing" or voice phishing – the act of using the phone to scam users into giving out their private information).

Social engineers also utilize SMS messaging (called "smishing"), create pretexting (invented) scenarios that force the target to respond, and will even resort to impersonation to gain access to a controlled building.

According to the George Washington University, here are the four phases of the social engineering lifecycle:

Preparing the ground for the attack:

- Identifying the victim(s).
- Gathering background information.
- Selecting attack method(s).

Deceiving the victim(s) to gain a foothold:

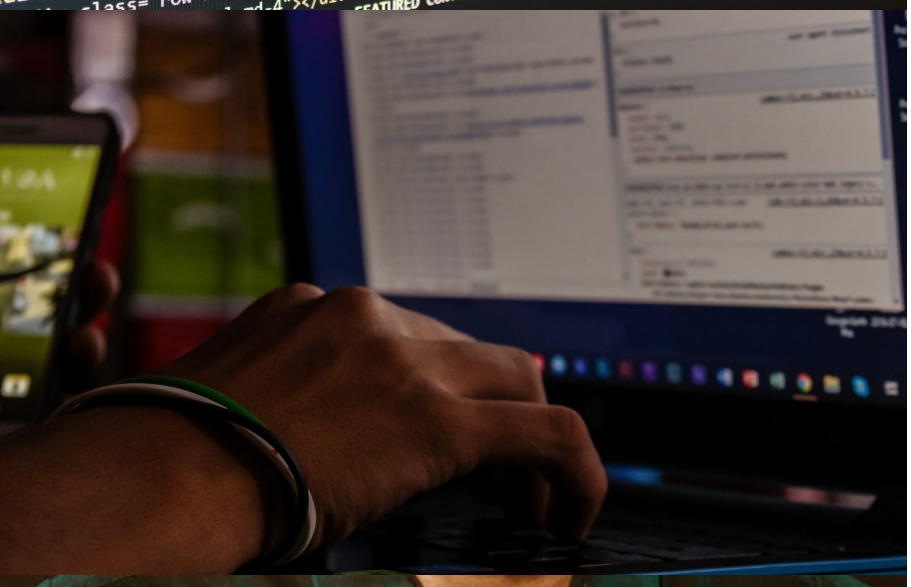
- Engaging the target.
- Spinning a story.
- Taking control of the interaction.

Obtaining the information over a period of time:

- Expanding foothold.
- Executing the attack.
- Disrupting business or/and siphoning data.

Closing the interaction, ideally without arousing suspicion:

- Removing all traces of malware.
- Covering tracks.
- Bringing the charade to a natural end.



The Four Phases of Social Engineering

Phase 1: Investigation

During the investigation phase, a social engineer will look into whom they want to focus on as their next target. Once they've determined the person they want to go after, they'll mine information about that person from any public sources (i.e. social media channels, company websites, etc.).

Phase 2: Hook

Once they've got enough information, the social engineer will initiate an interaction with their intended target. At this point, this could be a simple email, social media direct message, or a chance in-person meeting. During this initial ecounter, the social engineer will use the information they've gathered to start manipulating the target into doing what they want.

Phase 3: Play

The Play phase is when the social engineer will actually attack the victim. However, before they do, the social engineer continues engaging with their intended target, forging a stronger perceived relationship and deepening that trust they've built. Then, they'll attack.

Phase 4: Exit

After the social engineer has accessed what they need from the target, they'll disengage from the relationship they've built. The social engineer will also attempt to remove any traces of themselves from the victim's life.

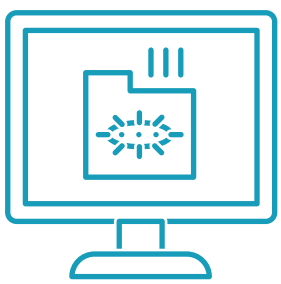
How Does Social Media Play a Role?

Social engineers gather information about their intended targets from any public sources. With such a prevalence in social media interactions in our society today, this is often the first place that a social engineer will go to mine data about the person they're going to target next.

This is not to say that social media is bad. What's harmful is not realizing how much personal data is actually being shared, which could be used for nefarious purposes. By using social media without carefully considering what we're sharing, we're making it easier for social engineers to find out information about us.

Whether it's on Twitter, Instagam, LinkedIn, or Facebook, we're constantly giving out enormous amounts of personal data!

Social engineers can use this information (and more) to their advantage and gather a lot more about you than you probably thought possible.



Let's take a look at some examples of things that people often share that could get them into trouble with social engineers:

- Posting pictures of pets or children (including names).
- Mentioning children's birthdays and/or ages (think twice before posting things like, "Happy 11th birthday to the sweetest kid I could have ever hoped for!", "Can't believe my little man, Aiden, is 9 today!").
- Tagging children in school pictures, or mentioning what school activities your children are doing. ("First day of Grade One at Lincoln Public School!", "So proud of Suzie's Parkway PS soccer team as they take gold!").
- Posting pictures or comments about your own birthday, wedding anniversary, job anniversary, or other significant dates.
- Posting content about new jobs you might be
- starting, or volunteer opportunities you may be involved in.
- Travel information, or checking in from hotels, restaurants, and/or airports.

Beware the "Fun" Games You See

Another way that we're giving out enormous amounts of personally identifiable information is engaging with or answering those internet games that often come across our social media feeds. Take, for instance, the following examples below.

In this scenario, you're asked to find your "Random birthday scenario" – a funny little story that explains what you supposedly will do on your birthday. Let's say that your birthday is March 15th, and you were born in 1979. By this game, your random birthday scenario is "Wrote a poem about Johnny Depp in California".

It may seem cute, but think about the information you're giving away with this game – anyone seeing your response post will know your birth month, the day you were born, and the last digit of your birth year. Combined with other information on the internet and various social media profiles, it's not that hard for threat actors to determine your full birthdate. And someone's birthdate is a key component for identity theft… just by playing a seemingly harmless game!

Even if you don't give away your birth month, zodiac signs are just as telling when it comes to finding out your birthdate. For instance, let's say (as in the previous example) your birthday is on March 15th. You're a Pisces (people born between February 20 and March 20), you're wearing a red shirt, and you're born on the 15th. So, your Sherlock Holmes Story is "The Problem of the Loquacious Turtle". Given that the Pisces zodiac sign only has one date in its range that has the number 15, it's pretty easy to deduce that your birthday is March 15th.

Birthdays, Name of Your Children, Street you Live on...

These aren't the only games out there, of course. But each of these "find your punk/goth/pirate/fairy/elf/Disney princess/etc. name", or "here's your dream date", or other similar games are all designed to mine personally identifiable information about you.

Birthdates, names of pets or children, street names that you've lived on, the names of your parents – these are all things that we might typically use as the answers to any security "challenge" questions we've set up on our accounts. Yet, because they're in game format, we often don't think twice about revealing this information that will ultimately help hackers!

How to Protect Yourself Against Social Engineers

Do your posts pass the "stranger test"?
A good way to answer this question is to think,"would I go up to a stranger on a bus, at a store, etc. and tell them what I'm about to post?" If the answer is no… don't post it.

Do your posts contain clues about responses to anyof your security "challenge questions" for any of your accounts? Don't use your favourite pet's name as a challenge question, then keep posting pictures of "your favourite dog, Cappy".

Are you giving away personally identifiable information?
Make sure your social media feeds don't have your full birthdate (month, day, and year) registered. Be careful when playing internet games that give away birthdates, street names, etc.

Are your posts showing off any particular habits or personality traits about you that would make you a target? Posting content around your passions and interests is great for social engagement, however, it's also great for social engineers, too. Be cautious about what exactly you're sharing, and make sure that those passions and interests can't be used to lure you into clicking on links later on.

Turn off Geotagging! When using your social media accounts, don't "check in" to restaurants, hotels, or airports. This helps threat actors know that you're not at home, and, if they're located in your area, they could potentially target not only your social accounts, but your physical goods and assets as well.

Set strict privacy settings for all your social media accounts you have, and don't respond to persona or account information requests.

Close old accounts you're no longer using.
Everyone's got that old email address from when email first came out. If you're still sporting an old account like RokerChik8@hotmail.com, or hotguy217@yahoo.com, it may be time to retire that email address.

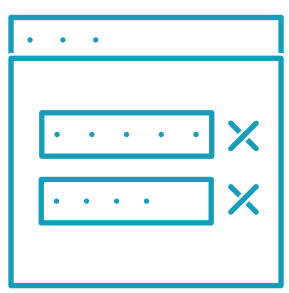
Change Your Password frequently!
Passwords can be hacked, even with the best of intentions in mind. It's important to change your passwords on a frequent basis.

Chapter 3:
Password Management

Human psychology says that we probably only remember 3-4 passwords at any given time. And yet, we have dozens of sites and accounts that we're signing into on a daily, weekly, or monthly basis.

What's the most common "answer" to this problem; something that most end-users are guilty of doing at least once? Unfortunately, the common "answer" to this problem is to re-use passwords, or create the same root password and just change the digits and/or symbols either before or after the root word. For example, choosing to use Pa$$word1234! for one of your accounts and then choosing Pa$$word2468! for the next.

These passwords are far too similar, and, from a security perspective, this is a massive risk to take. It's a solid bet that, if threat actors do get access to one of your accounts, they're going to try and use that same password (or similar variations) to access other accounts that may be linked to your email address.



Password Management Best Practices

When selecting your passwords, it's very important to ensure that it's not something that can be easily guessed. Experts suggest that you steer clear of using things like your favourite sports (or sports teams), favourite bands, favourite movie/characters, anniversary dates, birthdates, significant other/spouse's name, or names of your children or pets, as these are typically things we talk about the most, and things that are easiest to guess.

But selecting a strong password goes beyond just steering clear of things that could be easy to guess. In fact, experts these days are suggesting that, rather than using passwords, people should start creating passphrases to use.

What is a Passphrase?

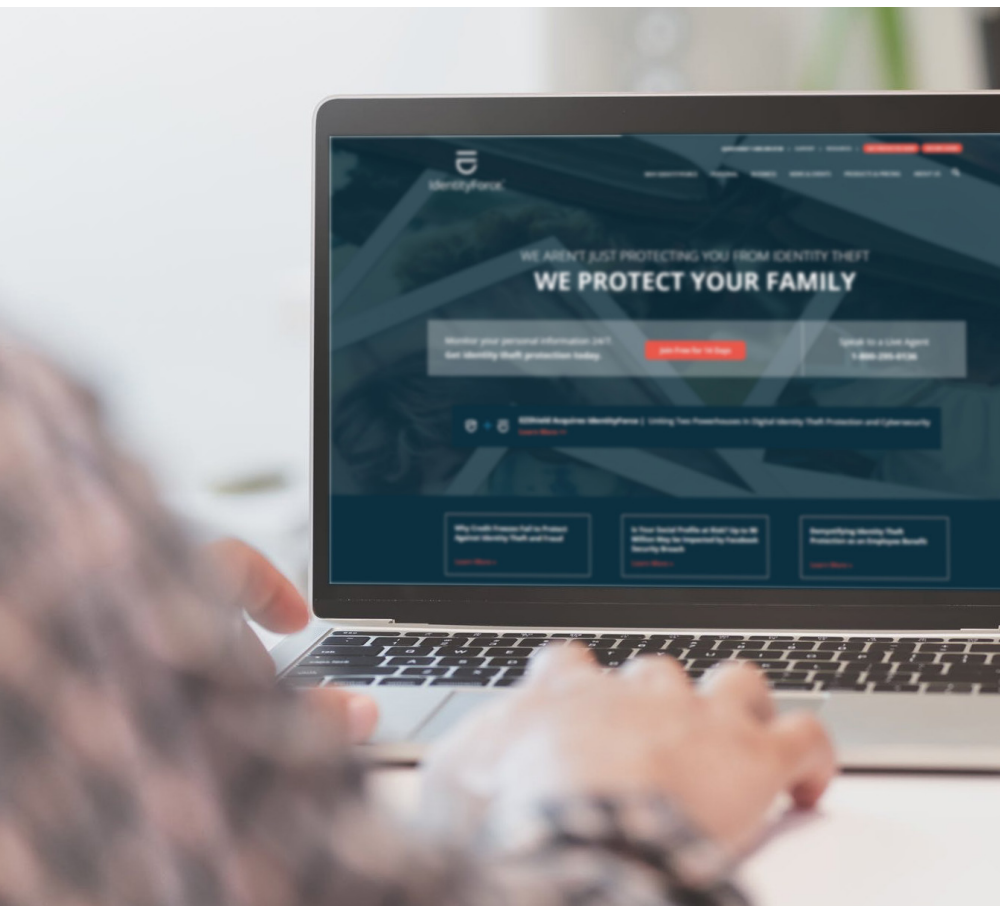
Simply put, a passphrase is three or four seemingly unrelated words that have special significance to the person creating it, but would be hard for others to associate or guess. For instance, using the objects people typically find on a desk as inspiration, a new passphrase could be PenPhotoStaplerPhone2020!

Five Ways to Secure Your Digital Life With Regard to Password Management

1 ***Never Reuse your passwords, and change them frequently!*** As mentioned, this is one of the best ways you can protect yourself and secure your digital life.

2 ***Avoid "Post it Note" security.***
You'd be surprised at how many times some of our technicians have gone to a client site to help them with some onsite work, and those people they're helping have a post-it note on their desk with their password written on it! It's very important to ensure that, if you do have trouble remembering your passwords, you aren't using "post it note" security. This leads to our third tip.

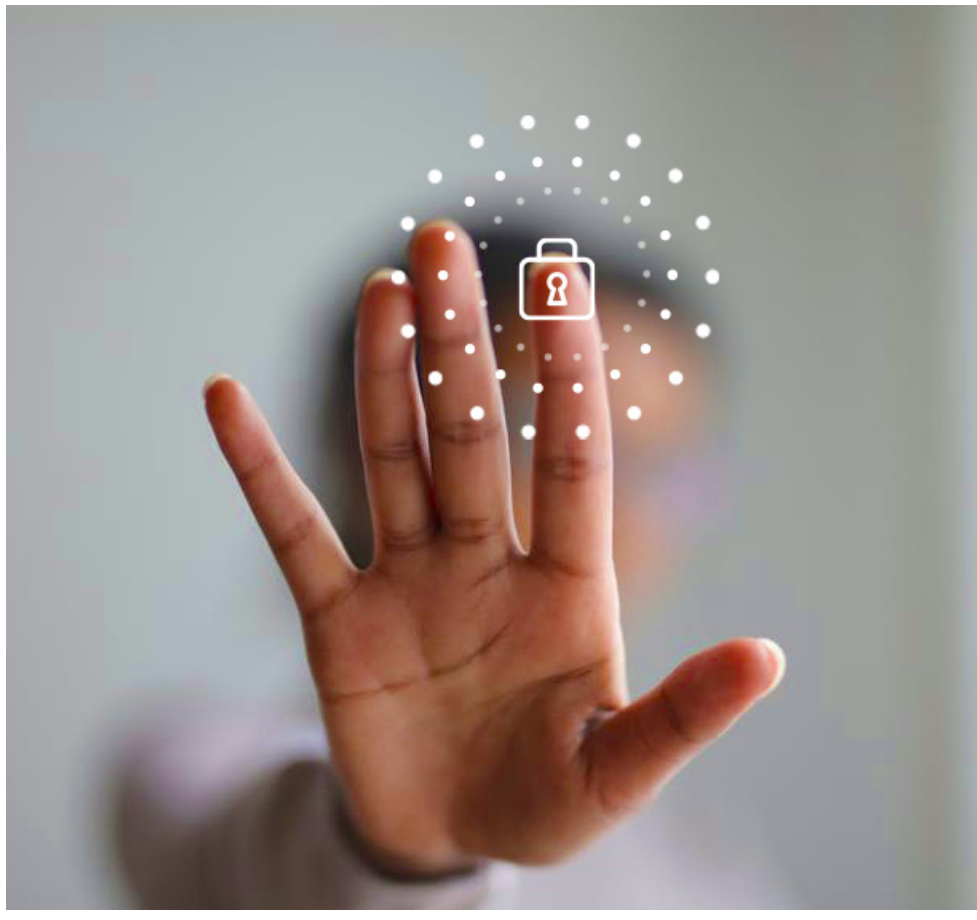
3 ***Use a Password Manager (like KeePass, Keeper, Dashlane, LastPass, etc.)*** Password Managers, like the apps listed above, allow you to store all your passwords in a secure location on your phone or online. This way, you only have to remember one password – the password for your Password Manager – and the other passwords are all there for you when you need them.



4 ***Consider an Identity Protection Service, such as IdentityForce, UltraSecure+Credit, or LifeLock Ultimate Plus, or similar.*** Identity Protection Services (like the ones mentioned above) can help you to proactively monitor whether or not there has been any suspicious activity with regard to your identity, as well as help you in the event that your identity is stolen and used for nefarious purposes. These kinds of services monitor internet activity on your behalf and warn you if your data has been leaked in a data breach, or if someone is trying to use your information and credentials to open a new credit card or social security number in your name – telltale signs that someone is trying to steal your identity.

5 ***Enable Multi-Factor Authentication (MFA) whenever possible. This is also called Two-Step verification.***

Multi-Factor Authentication (or MFA for short) is the process of presenting two pieces of authentication methods (like a password and your fingerprint, or a password and a swipe card, or a password and an authentication app on your phone) to prove that you are who you say you are. Enabling MFA adds an additional layer of security protection because it means that your password isn't the only thing needed to get into your account – a threat actor would also have to be in physical possession of your phone or your fingerprint (for example) to be able to access your data.



Chapter 4
Putting it All Together

3 Things To Remember to Keep Yourself Safe

First, it's important to make sure that you're educating yourself on the potential threats and risks that are out there.
Do a Google or Bing search on some of the latest phishing attacks, check out industry webinars and/or blogs (like the ones that *ProServeIT* has written) on the topic of cybersecurity.
These are good ways to educate yourself, but it doesn't stop there – be sure to share what you've learned with your colleagues, so that you're all participating in keeping your organization and your personal accounts safe.

Second, if you use social media, check the privacy settings on your social media accounts and make sure that they're set at levels you're comfortable with. Facebook, Instagram, and Twitter are notorious for changing or resetting various privacy settings whenever they do updates to the platforms, so it's important to do a continuous check on each of the platforms you use to ensure that your settings haven't been changed without your knowledge.

Third, updates those passwords on a regular basis! If you're using passwords that you've had for years, or if you're using the same password for multiple accounts, it's time to make a change. Consider using passphrases instead of passwords to ensure that you are making it much harder for threat actors to guess how to access your content.

PROSERVEIT

MAKING TECHNOLOGY TRANSPARENT

ProServeIT.com | Cloud@ProServeIT.com | @ProServeIT