CW technology

TECHNOLOGY & YOU

BEST IT PRACTICES

Advice from a Non-Technology Expert

Katherina Yavela
Marketing Coordinator

TABLE OF CONTENTS

AUTHOR'S NOTE

Katherina Yavela is the Marketing Coordinator at CW Technology.

A recent 2020 college graduate and new member to the CW team (as of June 2020), she brings passion, creativity, and resilience in growing our brand name, image, and awareness.

With an extensive marketing background and well-rounded set of experiences, Katherina has introduced a newfound perspective on marketing the IT and MSP industry. Her lack of a technical background doesn't stop her from learning and understanding the world of technology and the tremendous importance it holds, especially today.

At CW Technology, Katherina's role is building the brand across numerous marketing platforms, making the industry both relevant and reachable to all.

When not at work, Katherina enjoys reading, cooking, and learning Italian, which happens to be her fourth language!

INTRODUCTION

Are you someone without a technical background, and little to no knowledge of technology? Do you find yourself constantly Googling answers to your IT questions?

Don’t worry – you’re not alone. If fact, you’re someone like me! That’s right, I am no technology expert, and that’s why I have decided to share my advice with you on best IT practices.

WHY IT MATTERS

The world of technology can be overwhelming, even frightening at times...

Whether we care to admit it, as a society, we have become technology-dependent, and this has made us all - individuals and organizations alike - increasingly susceptible to any and all cyber-attacks.

No one wants to find themselves in a position where a single mishap could result in complete disaster.

In general, no one wants to be a position where do they not know what to do, especially when it comes to technology…

For this very reason, and from my experience, I have compiled the three, best IT practices for you to implement both in your personal and professional environment.

Technology is a blessing - let's not let it turn into a curse!

CHAPTER 1

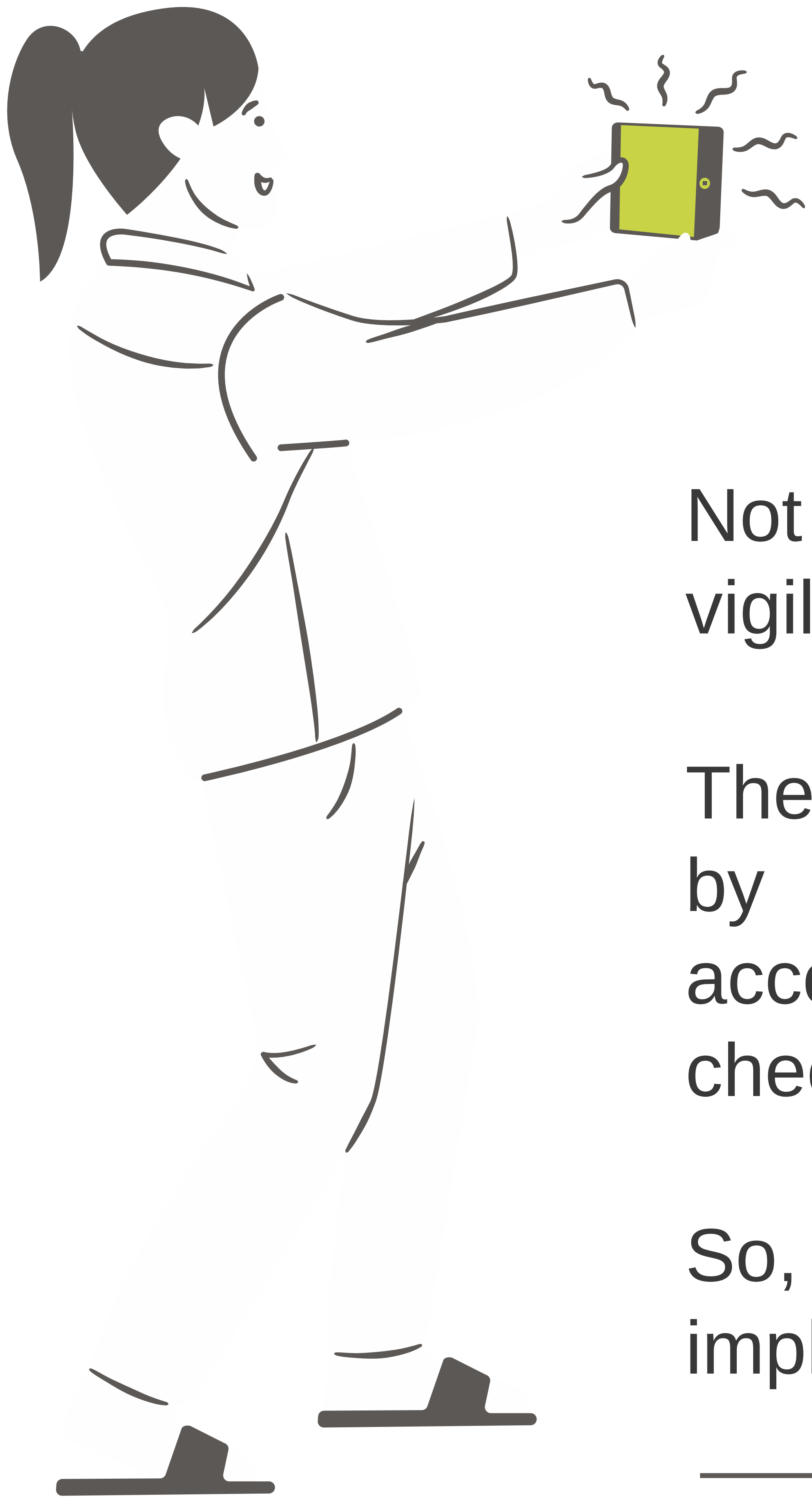
PROTECT YOUR ACCOUNT, PROTECT YOURSELF

Prior to working in this industry, I had no clue about additional security settings on all my personal accounts…did you?

In today's current climate, cyber security attacks are consistently increasing, and hackers search for people like you and me to gather intelligence on to exploit in their malicious schemes.

Did you know that we actually help them do that? Not purposefully, but sadly, without even realizing it. With every piece of information we put out on the Internet, from sharing our location and likes/dislikes, to online shopping, we practically hand ourselves over to cyber criminals.

Does that mean that we must quit social media and only make in-store purchases?



Not at all! What it does mean is we have to be more vigilant about protecting our personal accounts

The good news is organizations already help us do so by incorporating extra layers protection in our user account security settings. All that's left on our end is to check the box and update our account!

So, what are some of these security settings you can implement?

PASSPHRASE > PASSWORD

First and foremost, update your current password by changing it into a passphrase.

What is the difference?

A password is a single word made up of letters, symbols, and numbers, and unfortunately, is far from ideal in protecting your account.

We are all familiar with creating passwords, and we tend to make them short, hard to memorize, and complex; in many cases, people still re-use the same password for multiple accounts!

For this reason, passwords have a significantly higher chance of getting hacked…

In contrast, a passphrase is simply a collection of random words. Passphrases are easy to memorize, long and unique, and most importantly, protected by Multi-Factor Authentication tools and Password Manager tools.

MAKE THE RIGHT CHOICE

✗ 7$PONGEB0B

✓ SOUPWIRELEAF

So, if you haven't already, change your password! Or should I say… passphrase!

MFA SAVES THE DAY

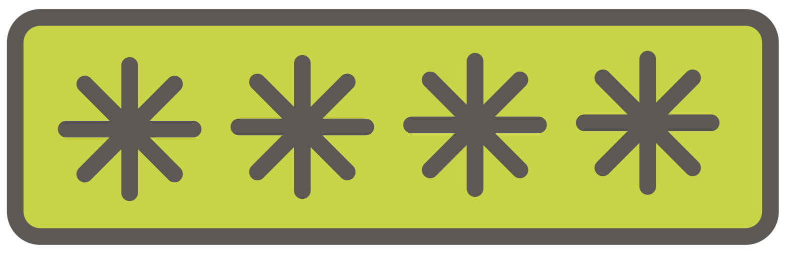
By selecting to MFA, or Multi-Factor Authentication, in your account settings, you have to provide two verification factors on your devices to log into your personal account.

For those unfamiliar with MFA (also known as Two-Factor Authentication), it is a tool that has a user provide two out of three factors when logging in.

These three factors include:

SOMETHING YOU HAVE

SOMETHING YOU KNOW



SOMETHING YOU ARE

By satisfying two out of these three factors, you decrease the likelihood of cyber security attacks and hacking.

The most common factor of MFA is an OTP or a one-time password: a 4 -8 digit code sent to you via email, SMS, or an authenticator application, such as **Duo Mobile** or **Google Authenticator**. On most platforms, such as *Facebook* and *LinkedIn*, you'll find these authenticator apps as the primary option when setting up your MFA.

If you have a social media account with little to no security settings enabled, chances are you or your friends have already been a victim of a cyber-attack and continue to be primary targets for another one...

MFA SAVES THE DAY

Think about it: have you ever received personal messages in your inbox from your *Facebook* friends, especially those with whom you rarely interact (i.e. post photos with, like their posts, etc.)?

Did those messages happen to have some enticing or even frightening message like, “You have to see this!” or “OMG! Is this YOU?!” with links to a *YouTube* or other *Facebook* URL?

By now you are probably aware that these were not ordinary, personalized messages, but scams targeting you via your hacked friends’ profiles. If you were someone like me who happened to interact with these, your profile ended up getting hacked just the same; from there, your account sent the same messages to your *Facebook* friends list, and so on and so forth.

Now, the fastest damage repair strategy was to change your password and write a public post, “My account got hacked. Don’t open any messages I sent to you!”

But, is this enough…? Unfortunately, no.

Sure, your post may have prevented some of your friends from making the same mistake as you did, but that’s about it.

Once your account has been hacked, the cybercriminal has access to everything: your email addresses, your answers to security questions, your phone number, your financial information, the list goes on...

MFA SAVES THE DAY

So, you see, a password change doesn’t do much to protect you from another cyber-attack…

Once you’ve regained access to your account, changing and verifying all your information is a start, but it too, isn’t enough. If a cybercriminal was able to hack your account before, chances are, they could easily do it again.

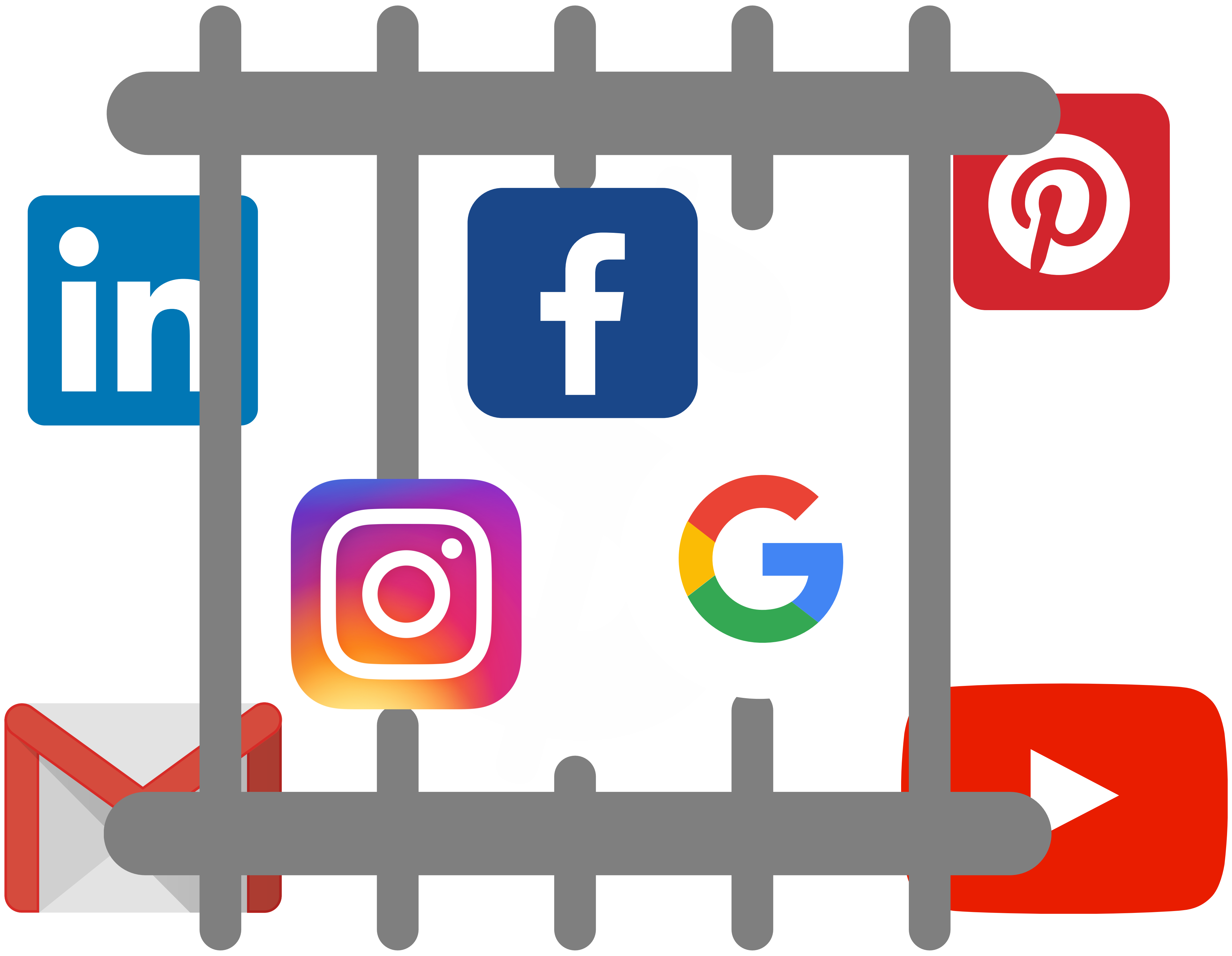
Keep in mind: we are living in the 21st century – an age of incredible, continuous technological innovation and advances. This only means that cybercriminals are becoming craftier and smarter with how they steal people’s information, especially with how much is shared on the Internet.

So, if you haven’t already, set up and enable MFA for all your accounts – personal and professional – for that extra layer of protection. Do it…do it NOW!

PUT PRISON BARS OVER YOU PROFILE

First, don’t take this literally: this doesn’t mean you should rarely go on social media quit the Internet entirely.

Second, this is the easiest and simplest step when it comes to protecting your online accounts. Next, go to your account settings right now and click on the security settings. From there, enable security and privacy controls as you seem fit, such as changing your account private or only visible to friends, versus public.



Lastly, always think before posting, whether it’s a photograph, your location, or any other form of personal information: the minute you share something online, it will be on there forever.

A general rule of thumb I recommend (and personally abide by) is, “If you don’t want it posted on a billboard on a highway, don’t post it!”

The more protection you have, the more secure your account is from cyber threats and attacks. That’s it, I told you it would be easy!

CHAPTER 2

DON'T GET HOOKED...

Let’s discuss phishing, and no, not the fun kind. Phishing scams have become the most common type of cyber security attacks, and they are not going anywhere...

To make matters worse, the COVID-19 pandemic is greatly responsible for the major surge: it has provided cyber criminals with a viable platform to persuade individuals in sharing their information, such as personally identifiable information (PII), intellectual property, and other valuable data.

Since the pandemic hit the United States last year:

1 in 4 Americans receive a phishing email scam related to COVID-19.

×3

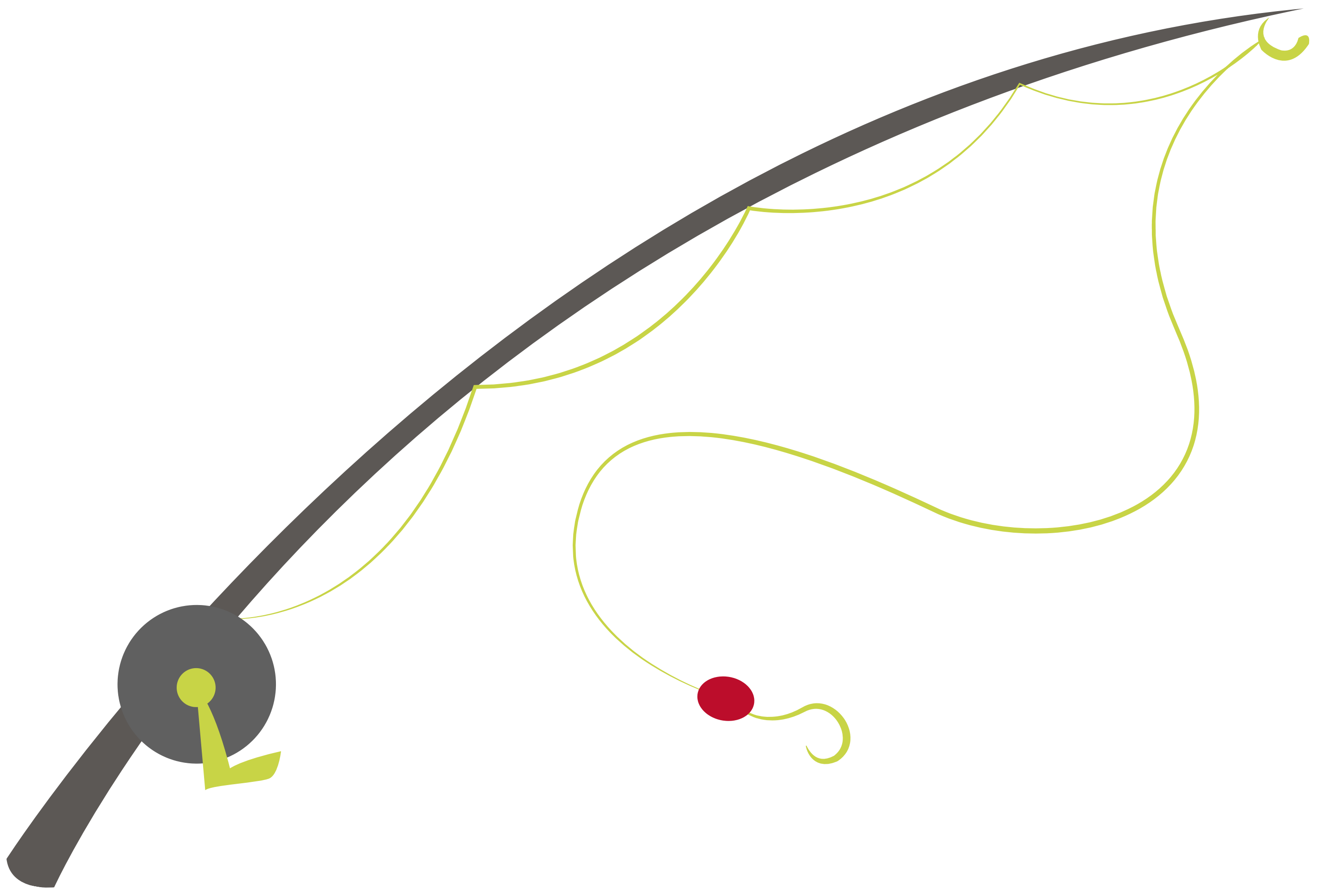
Users are three times more likely to click on a pandemic-related (phishing) email.

Over 240 million COVID-19 related phishing scams are sent daily.

One of the primary reasons why COVID-19 is responsible for the increase in phishing scams is the shift to remote work.

Since most of us no longer work in an office, we don’t have an IT department to run to and fail to differentiate between what’s real and what’s a scam.

Whether your company regularly hosts employee security training or not, in the end, it is solely up to you to not get hooked. Believe it or not, even working for an IT company doesn’t automatically mean I am safe from phishing scams. In fact, in the last several months, I have come across 4 “phishy” emails, of which 2 were targeted phishing scams!



At this point, you might be thinking, “Okay, but how do I identify what’s a scam and what’s an actual email from my boss?”

Good question, and believe me, it’s easier than it seems! As creative and smart cyber criminals can be, they cannot control every aspect of the email they send – this is where you come in!

There are numerous preventive measures you can take to identify a phishing email, but because there are so many, at least a third of people noted they proceed to engage with an email after taking a single step...

Even if the first 3 steps you take check out, that doesn't mean it isn't a phishing email! A common example is an email sent from a work colleague, especially from a supervisor or manager.

64% of employees stated they open and interact with an email from their boss, and that is exactly what cyber criminals count on!

Remember how I mentioned I caught a phishing scam? Well, it came from my boss! That's right: the cybercriminal attempted to phish for information by making it seem as if my boss required me to conduct a company purchase…

It was by going through every, single one of those preventive steps that I successfully identified a phishing scam.

There are many cases where it isn't that simple to identify a phishing email. Let's say you did go through every step, but you are still unsure whether the email is real or a scam.

What now?

First and foremost, do not interact with it in any. Instead, delete and report it immediately. If you have doubts that it may be important company information, simply take a screenshot of the email in your inbox and contact your supervisor right away.

Remember, it is always better to be safe than sorry!

TOP PREVENTIVE MEASURES TO IDENTIFY A PHISHING EMAIL:

✓ **Determine if the sender’s email address is unknown or fake.**

Example:
securityamazon@securityamazon.com

✓ **Identify if the introduction is too generic (i.e. does not include your name).**

Example: Dear Customer

✓ **Search for multiple grammar mistakes and common spelling errors.**

Example: "your" vs. "you're"

✓ **Observe if there is a suspicious call to action, such as to your share personal information or to click on a suspicious link.**

Example: "Update your billing information now.”

TOP PREVENTIVE MEASURES TO IDENTIFY A PHISHING EMAIL:

✓ **Identify if there is any threatening language.**

Example: “Failure to update your billing information will result in immediate account termination.”

✓ **Hover over any links to see if the URL makes sense.**

Example: “Amazon.com” vs. “evil.com"

✓ **Do not click to download any suspicious attachments.**

Example: “Download the form to update your account information.”

✓ **Identify if the sender’s signature looks fake.**

Example: Wrong font, size, color, etc.

CHAPTER 3

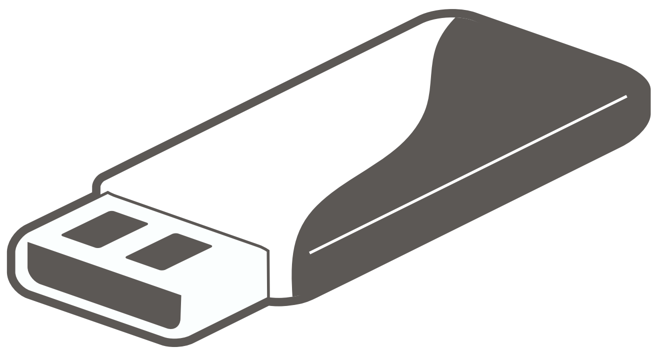
BACKUP, BACKUP... BACKUP!

It seems like such a simple, basic task that should be a habit by now, but the fact is, majority of people still forget to do it! You never know when your device could break, your network could crash, or a disaster could occur.

Data backup is not an option - it's a necessity! Companies have made it a part of their Business Continuity Disaster Recovery (BCDR) plan, as it plays a crucial role in a business's continuity and functionality.

Again… data backup is not an option - it's a necessity! Just like a business, no one wants to lose all their valuable data, whether it is personal information or even all photographs saved on our camera roll.

There are several, simple ways you can back up your data:



HARDRIVE

Backup all of your existing files and information from your laptop or workstation and copy them onto a secure hard drive.

ONLINE SECURE STORAGE

Don't have a hard drive? No problem! Backup all of your existing files and information through a secure online storage service, such as Google Cloud and Barracuda Cloud Storage.

And remember, as I have shared with you, share your backup practices with work colleagues, employees, friends, and family - help create a safer place for all online!

CONCLUSION

At this point, hopefully you not only have a better understanding of technology, but likewise feel more comfortable and secure using it for your personal and professional needs.

In any case, it is important to remember that the world of IT and technology is constantly evolving, so be sure to stay updated and continue implementing best security measures.

CW Technology makes technology easy. If you'd like to learn more about cyber security, or you simply need help in determining what are the optimal protection services for you, CW Technology is here to help!

Contact us today to discuss how we can implement the optimal security processes and tools for you!