Hacked, Now What? reveals how people—not just tech—are key to cybersecurity. With real examples and practical tips, Nathalie Claes shows how to spot risks, build a security culture, and protect your business from digital threats.

Hacked, Now What? Protect Your Business From Cybercriminals

By Nathalie Claes

Order the book from the publisher Booklocker.com

https://booklocker.com/books/14156.html?s=pdf

or from your favorite neighborhood or online bookstore.

Nathalie Claes

HACKED, NOW WHAT?

Protect your business from cybercriminals

Print ISBN: 978-1-959622-63-5
Ebook ISBN: 979-8-88531-964-5

Published by BookLocker.com, Inc., Trenton, Georgia.

Cover design: Armée de Verre Bookdesign
Illustrations: Jef De Cat
Picture author: Nouchka De Maeyer

BookLocker.com, Inc.
2025

First Edition

Library of Congress Cataloging in Publication Data
Claes, Nathalie
Hacked, Now What? Protect Your Business From Cybercriminals by Nathalie Claes
Library of Congress Control Number: 2025900676

DISCLAIMER

This book details the author's personal experiences with and opinions about cybersecurity.

The author and publisher are providing this book and its contents on an “as is” basis and make no representations or warranties of any kind with respect to this book or its contents. The author and publisher disclaim all such representations and warranties, including for example warranties of merchantability and cybersecurity advice for a particular purpose. In addition, the author and publisher do not represent or warrant that the information accessible via this book is accurate, complete or current.

The statements made about products and services have not been evaluated by the U.S. government. Please consult with your own legal, accounting, medical, or other licensed professional regarding the suggestions and recommendations made in this book.

Except as specifically stated in this book, neither the author or publisher, nor any authors, contributors, or other representatives will be liable for damages arising out of or in connection with the use of this book. This is a comprehensive limitation of liability that applies to all damages of any kind, including (without limitation) compensatory; direct, indirect or consequential damages; loss of data, income or profit; loss of or damage to property and claims of third parties.

You understand that this book is not intended as a substitute for consultation with a licensed medical, legal or accounting professional. Before you begin any change your lifestyle in any way, you will consult a licensed professional to ensure that you are doing what’s best for your situation.

This book provides content related to cybersecurity topics. As such, use of this book implies your acceptance of this disclaimer.

Content

CHAPTER 2.

The Nigerian Prince

Attention: The Managing Director

Dear Sir,

Urgent Business Proposal

We currently have thirty million US dollars which we got from over inflated contract from crude oil contract awarded to foreign contractors in the Nigerian national petroleum corporation (NNPC). We are seeking your assistance and permission to remit this amount into your account. Your commission is thirty percent of the money.

Please notify me your acceptance to do this business urgently. The men involved are men in government. More details will be sent to you by fax as soon as we hear from you. For the purpose of communication in this matter, we may have your telefax and telephone numbers including your private home telephone number.

Contact me urgently by replying to this email.
Thanks for your cooperation

Yours faithfully
Prince Jones Dimka
Lagos Nigeria

No doubt this mail has already been in the mailbox of every reader of this book, one way or another. A Nigerian prince who promises you a fantastic business deal, a person who wants to send you an inheritance, you unexpectedly won a large sum of money with the lottery, ... Today, anno 2024, you can hardly believe that these mails ever work. Unless you are a digital illiterate, like my grandmother who has never seen a personal computer up close.

But roughly 25 years ago, when the PC made its appearance in most SMEs and with it the connection to the Internet, this was not at all out of the blue. People were used to working with a typewriter, working with a computer was previously reserved for a select group of people who were allowed on the mainframe (*remember* punch cards). A whole new world opened up, positive but certainly also with negative sides.

Although today we still receive the mails from that handsome Nigerian prince with too much money, fortunately they end up in our "junk mail" folder very quickly. Most of the employees in companies I support never open it, so it's safe there. But by now, we have also been trained to recognize these, often clumsily drafted, language-erroneous emails and delete them immediately. Story over, you'd think.

Unfortunately, phishing has also evolved. The mail from 25 years ago doesn't work today, but new ways have been developed to trick people.

This chapter is about how to train your company to become super strong in security, ready to tackle any unexpected digital threat and come out of it stronger.

WHAT CAUSES PHISHING?

Many businesses today are at risk of falling victim to a phishing attack. Although the press mainly reports on the major ransomware attacks, where a company's data is encrypted and only released after paying a

very large sum of money, phishing (fraudulent emails) is often the first step.

Ransomware

Ransomware is similar to a thief breaking into your home, putting all your valuables in a safe, and then taking away the key. In the digital world, ransomware "takes" your computer files hostage by encrypting them, leaving you unable to access them. Then the attacker asks for a "ransom" (often in the form of bitcoin or another cryptocurrency) in exchange for the key to unlock your files.

This is a form of cybercrime where your own data is used against you as leverage.

SHOW ME THE MONEY

The reason why businesses are so vulnerable can be traced to two major factors.

The first reason mainly has to do with inadequate or improper investment in information security infrastructure. Let's face it, the terms above already sound fairly futuristic, but we all (at least me anyway) get a little anxious when the IT manager has to come and present his budget. There is a juggling of terms and abbreviations that has no name. Let alone fully understand what all those things are for. So, when the good guy says we need the latest new firewall or the latest new *intrusion detection* system, he is taken at his word. The question, of course, is whether what is recommended is the right thing for your organization, for your specific circumstances, based on the risks your organization faces. The latest new firewall may not necessarily be the right one for your circumstances.

Intrusion detection

An Intrusion Detection System (IDS) is like a security system for your business, but for your computers and your network. Just as an

alarm system protects your business premises from burglars, an IDS protects your digital environment from unwanted intruders.

Firewall

A firewall acts as a protective barrier between your internal network (for example, your company computers) and the outside world (Internet). It blocks unwanted traffic and lets only authorized communications through. Just like a doorman who lets in only authorized people , a firewall uses rules to determine what traffic is allowed and what traffic should be blocked.

Furthermore, based on recent research, there is still too little investment in cybersecurity. I can already hear every CEO and business manager screeching now, because quite a bit of money is being spent on IT. The challenge in the IT field, and by extension the cybersecurity field, is that development does not stand still. What is the cutting edge today is outdated tomorrow. Cybercriminals are constantly looking for new ways to make their move, so cyber security solution providers must also continue to invest and stay one step ahead. And that's what you pay for. Of course, you must always look for a good balance between investing in your business (sales, production, after-sales service) and securing your business. What's important here is that you at least get well informed and that you yourself also try to make the trade-off between what is really necessary and just nice to have.

THE WEAKEST LINK

I frequently come into organizations where there is absolutely no investment in providing proper training to employees. Providing the right training allows employees to better recognize signs of potential risks. Very often I see companies that cobble together a PowerPoint presentation, put it in a learning platform or their intranet and require their employees to attend it once a year - impact nil. Information security training must be tailored to your target audience, which means providing

different training. An IT employee needs different training than the receptionist or the financial employee. Management and executives need something completely different. *Death by PowerPoint* is real. Make the training interactive, alternate physical training with online forms, provide quizzes, and use real examples from the company. There is nothing like analyzing information about security incidents, finding out the reason and then providing training about it.

It is important that employees make the switch from reactive to proactive information security behavior. You want to get to the point where employees signal when they've received a strange mail. Now you often only know after the fact, when people have already clicked, that there was suspicious mail in the mailbox. Recognizing these signals requires training. Training that addresses three factors:

- What is staff knowledge on this topic?
- How do they think about it
- So how do they behave?

So, this type of training should best respond to personal experiences and use current events. A PowerPoint presentation that employees can scroll through (we all know them) is insufficient. By providing comprehensive training, you can keep employees abreast of current threats, you can teach them how to recognize signs, and thus everyone contributes to the security of company data

You don't have to produce this training on your own, there are plenty of companies on the market that can help you with a customized awareness *program*, either online or physically at your place of business.

No matter how you spin it, no matter how much you bet on all the technological gadgets, your employee is still a human being. And people want to do good and are triggered by all sorts of emotional things that are not always in your control. So why not arm them properly?

PORT OF ANTWERP (2013 - 2014)

INCIDENT: Criminal organisations worked with insiders in companies operating in the port of Antwerp. These insiders helped hackers gain access to sensitive information about container locations and security data, which was then used to smuggle drugs.

CAUSE: The attackers used insiders to steal critical information via keyloggers and screenshots, allowing criminals to intercept containers of illegal drugs before the legitimate owners arrived.

IMPACT: This led to the theft of multiple containers of cocaine and heroin, causing significant financial and security problems.

Keylogger

A keylogger is a type of software or device that keeps track of what someone types on a keyboard. It can be used by cybercriminals to secretly steal passwords, credit card numbers or other sensitive information.

The word "keylogger" comes from "key" (key) and "logger" (someone who records something). It's like a digital spy that records every key you press and transmits it to whoever installed the keylogger.

Keyloggers can get onto your computer or device in a variety of ways, such as through an e-mail attachment, a fake website or even by physically attaching a small device to your keyboard. So, it is important to properly secure your computer and be careful what you download or open.

HOW DO YOU RECOGNIZE A PHISHING EMAIL?

In today's digital world, where email plays a crucial role in business operations, knowing how to spot phishing emails is indispensable for any

business owner. These fraudulent messages designed to extract sensitive information can have serious consequences for your business.

First, it is essential to critically examine the sender of each e-mail. Phishers may pose as trustworthy entities, but often subtle discrepancies in the e-mail address betray their true intentions. Distinguishing these nuances requires a watchful eye.

Next, be vigilant for unsolicited attachments or hyperlinks. These are often embedded in the e-mail and, once opened or clicked, can spread malicious software. Therefore, it is crucial to be careful when opening unknown attachments or following links from unexpected sources.

Phishing emails often stand out because of their language and design. They may contain spelling mistakes, grammatical errors or an unusual layout. An e-mail that looks unprofessional may be an indication of a phishing attempt.

A common tactic used by phishers is to create a sense of urgency. By threatening immediate consequences, such as closing an account or imposing deadlines, they try to manipulate the recipient into acting quickly and without thorough consideration.

If there is doubt about the authenticity of an e-mail, it is advisable to contact the alleged sender using known, reliable contact information. In other words, you don't use the contact information provided in the email, but you use the information you yourself have. This helps to verify the authenticity of the request without being at risk.

In summary, recognizing phishing emails requires not only technological tools, but also an alert attitude and critical thinking skills.

WHAT'S IN A NAME?

I have been active in the world of IT for about 20 years now, and I continue to be puzzled by IT terminology. It sometimes seems like there is a club of IT experts hidden somewhere, with a very high geek content (*no offense*), who make it a sport to come up with the craziest names. Just to make things difficult for us ordinary professionals. All kidding aside, let me explain exactly what we mean.

- *Phishing*: phishing involves sending fraudulent emails that trick recipients into sharing their personal, financial or security information.
- *Smishing*: *smishing* (a combination of the words "Smsing" and "phishing") involves an attempt by scammers to obtain personal, financial or security information through a text message.

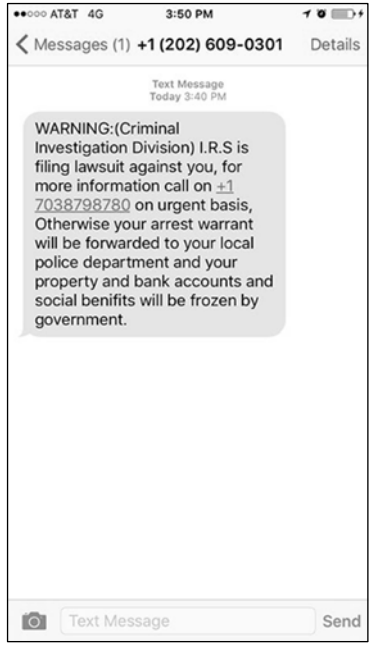


Figure 1. Example of a fake message notification (Source: proofpoint.com)

- *Vishing*: in *vishing* (a combination of the words "voice" and "phishing"), scammers attempt to grab personal, financial or security information over the phone.

- *Spear-phishing*: *spear-phishing* is a subset of phishing. Whereas phishing is employed to reach the widest possible audience in the hope that one fish bites, *spear-phishing* targets very specific recipients. In *spear-phishing*, cybercriminals target one specific person, often high up in an organization, whom they want to deceive. This form of phishing is often preceded by a lot of research by the criminals in order to get to know the person well and know what the triggers are that they respond to.
- *Whaling*: similar to *spear-phishing*. Cybercriminals focus on a big fish (*whale*) in an organization. Often this is someone in top management who has access to a great deal of confidential and sensitive information. Similar to *spear-phishing*, cybercriminals put a lot of time into researching the person in question beforehand.

WHAT HAS CHANGED?

The chances of becoming a victim of phishing, as cited earlier, are much higher today than they used to be. This is because companies now store much of their important and sensitive information in the cloud. In recent years, many companies have moved to these new digital ways of working. They are using "the cloud" more to make their processes more efficient and to make better use of their data. Recent studies show that it is expected that large enterprises will have about 60% of their operations in the cloud by 2025.

During the pandemic, the use of the cloud was essential for companies to quickly transition to working from home. But these benefits came at a price: an increased risk of cyber-attacks, including phishing. The increase of data in the cloud has been accompanied by an increase in data

breaches. Research shows that the number of data breaches worldwide more than tripled between 2013 and 2021. Experts expect this trend to continue, with an increase in serious attacks via the cloud.

E-mail remains one of the main ways phishing attacks are carried out. About 1 in 99 emails is a phishing attempt, and 30% of these emails are actually opened. In addition, attacks via social media and collaboration platforms are also prevalent. During the COVID-19 pandemic, the number of phishing attacks increased significantly. Globally, since 2020, 81% of organizations saw an increase in email phishing.

The threat of phishing is unlikely to diminish anytime soon. The World Economic Forum sees "widespread cybercrime and cyber insecurity" as one of the biggest short- and long-term global risks. Phishing attacks make up a large portion of all cyber-attacks, which means businesses cannot ignore them.

Phishing attacks used to primarily target e-mail, but now attackers are also using compromised websites and collaboration apps. This shows that attackers are adapting their methods to how defenders respond. Password protection alone is no longer enough.

Despite many digital means of communication, e-mail remains widely used worldwide. Therefore, it is not surprising that email remains an important channel of attack (in cybersecurity terms, attack vector) for cybercriminals, alongside Web applications. According to Verizon's Data Breach Investigations Report, Web applications and e-mail are the top two vectors for data breaches.

Verizon's Data Breach Investigations Report (DBIR) *is a comprehensive annual report that provides in-depth analysis of data breaches and cyber incidents around the world. This report is one of the most authoritative and comprehensive sources for information on cyber threats and security incidents.*

The DBIR is compiled by Verizon, a leading global provider of broadband and telecommunications services. Verizon has a specialized arm, Verizon Business Group, which focuses on enterprise customers and provides cybersecurity solutions. The DBIR is the result of collaboration between Verizon's cybersecurity experts and data analysts, as well as contributions from external partners such as law enforcement and other security companies.

The DBIR provides a detailed analysis of thousands of confirmed data breaches and security incidents that occurred over the past year.

The report is based on a vast amount of data collected and analyzed, providing reliable and representative insights into the current state of cybersecurity.

Moreover, the report covers multiple sectors, allowing companies in different industries to find specific and relevant information applicable to their situation.

In addition to providing analysis and trends, the DBIR also offers concrete recommendations and best practices that companies can implement to strengthen their security.

The report is known for its thoroughness and objectivity, making it a reliable source for security professionals, policymakers and business leaders.

DBIR's findings allow companies and their employees to better understand where the biggest threats lie and how to prepare and protect themselves.

Cybercriminals are getting smarter in their methods. For example, they now use automated text-to-speech systems and audio-deepfakes for *voice phishing* or *vishing*. They build complete organizational charts of companies by gathering information from platforms such as LinkedIn, then send targeted text messages.

In *De Morgen* of February 6, 2024, a full article was devoted to an employee of a multinational company who paid 24 million euros to scammers who used deepfake technology during a video conference. This video conference followed an email that the employee did not quite trust. The videoconference had then won him over after all.

Deepfake

Deepfake is a technique in which videos or photos are manipulated using artificial intelligence to make it appear as if someone is doing or saying something they did not actually do or say. It is like putting on a mask of someone else, but in this case it is done digitally.

For example, in a deepfake video, a celebrity may appear to say something he or she never said, or someone appears in a video when in reality he or she was not there. This can be used for humorous purposes, but unfortunately also for deception, such as spreading fake news or damaging someone's reputation.

Malware kits on the dark web allow even criminals with little technical knowledge to carry out sophisticated attacks. The malware economy functions like a legitimate business, where you can buy malware and pay someone else to run a phishing campaign for you. The WEF's Global Risks Report notes that advanced cyber tools allow attackers to operate more efficiently. These days, there is even Phishing-as-a-Service, where you pay some sort of monthly fee to a cybercriminal to carry out phishing attacks. All can be found on the dark web.

Dark web

The dark web is a hidden part of the Internet that is not accessible through normal search engines such as Google. You can compare it to a secret room in a large building. To get in, you need special keys or software, such as a program called Tor.

Illegal activities are often carried out on the dark web, such as the sale of stolen data, drugs or weapons. But there are also those who use it for legitimate reasons, such as activists or journalists in

> *countries with strict censorship. So, it is a part of the Internet where anonymity is central, but which is often abused for criminal purposes.*

Despite large investments in cyber security, this may be insufficient. The number and complexity of cyber-attacks are increasing. The change in business models, such as working from home and using the cloud, increases the risk. Many organizations are struggling to keep up with these changes.

The human element is often the weakest link in security. Phishing plays on human error. According to Verizon's report, 74% of all breaches are related to human error, including the use of stolen login credentials and social manipulation (in cybersecurity terms, social engineering). This highlights the importance of cyber security awareness and training.

HOW DO YOU WEAPONIZE YOUR ORGANIZATION?

To stay resilient in the digital world and outsmart cyber-attacks and phishing, companies really need to work on their digital muscle. Think of this as a kind of fitness routine for your cyber security. It's not enough to just do some individual security things. You need an overall plan that protects your business from devious cybercriminals.

Security fitness means being ready for anything, good or bad. It gives you the power to attack any cyber threat head-on and win.

In summary, here are four things to keep in mind to ensure that your company remains resilient in the world of information security.

The four keys to security fitness:

- *Prevention*. Use strong spam filters to block phishing emails and train your team on fake phishing attacks. Update your software regularly and use antivirus programs.

- *Containment*. If you do face a cyber-attack, make sure you can respond quickly by isolating the infected system. Secure your backups offline
- *Make your employees aware*. Teach your employees how to recognize an attack and how to respond.
- *Test and practice*. Test your contingency plans regularly to make sure you are ready for a real attack.

Make sure your security solutions work well together, both in the cloud and on your network and *endpoints*. Protection of *endpoints* is essential to tackle phishing.

You absolutely don't need to be a cybersecurity expert to protect your business. Use smart technologies, such as AI, to build a strong defense. One simple trick is to randomize email addresses in your company so that phishing emails are less likely to reach the right person. By randomize I mean that you move away from the standard firstname.lastname@companyname.com , but switch between this format and, say, name@companyname.com , and produce other variations on this. After all, it is super easy to go to a company's website and find an e-mail address (yes, there are tools for this too, but sometimes they are just on the contact page), then apply this to all employees in the company and set up a major phishing attack.

In short, be proactive, stay alert and work smartly together to protect your business from today's cybercriminals!

The steps to super security:

- *Make security a team sport*. Everyone in your company should know the importance of working together against cyber-attacks. Train your team to spot suspicious emails and weird software and report it immediately! By creating a company culture where everyone is alert, you will boost your security force tremendously. Make a "wrong click" negotiable!

- *Find your weaknesses*. Check your systems, processes and technology for weaknesses. Know what your external risks are; make sure you don't have a single critical system that could go completely down if attacked. Use risk assessments to prioritize your defenses.
- *Get management involvement*. Security is not just something for your IT department. You need the support of your company's top management.
- *Get the right tools*. Make sure you have enough people and resources to respond quickly to unexpected cyberattacks. Also consider partnering with an outside party; they have the knowledge.
- *Start thinking about security*. Set strict security rules and make sure everyone follows them. Don't wait until something goes wrong. Immediately develop a plan to deal with incidents.
- *Use threat intelligence*. Good info on cyber threats helps your team respond better to attacks. Provide automated monitoring of your systems in real time
- *Choose simple, flexible technology*. In cybersecurity, simplicity is important. Use technologies that are easy to manage, such as multifactor authentication (MFA).

Multifactor authentication

With MFA, you use not one, but multiple ways to prove that it is really you trying to access something important, such as your e-mail account or bank account. The first "key" is something you know, such as your password. The second 'key' may be something you have, such as a code sent to your phone. And sometimes there is even a third "key," such as your fingerprint or facial recognition - something unique to you.

By using all these "locks," you make it much harder for others to get to your important stuff. Even if they steal your password, they still

need the other "keys. It's like guarding your treasure chest with a password, a secret code and a magic spell that only you can cast!

- *Secure everything*. Use multi-layered security: user MFA, *endpoint* detection, email security, protection of web traffic and cloud apps, and ensure secure data.

Endpoint

Imagine a large house with many doors and windows. Each of these doors and windows is a way for people to get in and out. In the world of computers and the Internet, we call any device that can connect to a network - like your laptop, smartphone or even your smart refrigerator - an endpoint*. It's like a door or a window in your house.*

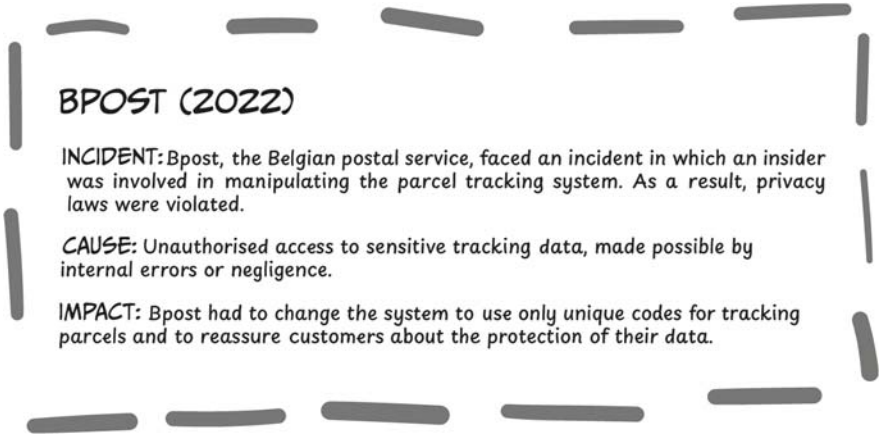
Just as you want to make sure that every door and window of your home is properly secured to prevent burglars from entering, you also need to make sure that every endpoint *is secured in a computer network. That means you want to make sure that every device that connects to the Internet is well protected from viruses, hackers and other bad things on the Internet.*

So, an endpoint *is a fancy word for any device that can connect to a network. You need to make sure each of these "digital doors" is properly locked!*

Of course, as a non-IT manager, you cannot protect the organization alone. You need the support and input of your IT team and/or IT security team. Even if you don't have an IT team, it's important to know what questions to ask your IT vendor. After all, you can't outsource your problems and responsibility; you remain responsible for what that partner does for you. However, in a lot of companies I see that this reflex does exist, you call on a partner and then you shouldn't care about anything. Nothing could be further from the truth; you remain responsible for checking that your partner follows your guidelines and makes every effort to deliver the promised service.

What key questions to ask your IT team:

- When can we expect an attack?
- Are we ready to detect every threat?
- Where are we most vulnerable?
- How quickly can we respond and recover?
- Are we getting better at security?



WHAT'S COMING NEXT?

The end is, unfortunately, not yet in sight. We live today in a world that is constantly changing, new technologies coming our way, weird political states, ... And we live in a world that is becoming more and more digital, we all accept, without thinking, the terms of the apps we install. But we have no idea where the information goes, whether we can trust the parties. In short, we are often just unaware.

We dive into five key trends that will have a major on how companies should approach their digital security. These five trends highlight the importance for companies to be proactive in their approach to cybersecurity. It's not just about installing the latest security software; it

also requires a culture of awareness and ongoing education about the latest threats and best practices.

Artificial Intelligence (AI): two-edged sword

As I wrote earlier, AI is a real gamechanger in both cyber-attacks and cybersecurity. For attackers, it means setting up easier and smarter attacks. They can now use AI chatbots to create credible phishing emails without language errors and personalize them with data collected online. On the defense side, AI helps identify and stop threats faster. Machine learning algorithms can be trained to identify suspicious emails, which is a crucial step in preventing phishing. There is growing evidence, both from studies and real-world examples, which shows how generative AI technologies are being used for social engineering attacks. Cybercriminals are exploiting generative AI to fabricate phishing emails, chatbot interactions and voice impersonations that appear surprisingly real. These AI-assisted attacks exploit the unique ability of generative AI to create authentic-looking content that can bypass traditional security controls.

The war between Russia and Ukraine: a cyber front

Since the outbreak of war between Russia and Ukraine in 2022, the world has seen an increase in targeted cyber-attacks, particularly against Ukraine. These attacks include phishing emails related to the conflict, such as messages about humanitarian aid. These emails are used not only to scam, but also to spread malware. This highlights the need for businesses to be extra vigilant for emails related to current world events. Moreover, we are also seeing these targeted attacks toward countries supporting Ukraine. For example, we saw a huge increase in attacks on Belgium's critical infrastructure (hospitals, energy suppliers, water companies, etc.) when the promise was made to send F-16s. This seems to be time-bound, the question is whether with increasing unrest worldwide, cyber-attacks will also become an unstoppable tool of war.

The Log4Shell vulnerability: a warning sign

In late 2021, a major security vulnerability became known in Log4j, a widely used software library. This vulnerability, known as Log4Shell, potentially gives attackers full access to affected servers and has been assessed as a critical vulnerability. It illustrates how important it is for companies to keep their systems up to date. It also shows how essential it is to be aware of the software and tools used in the organization.

Politically motivated cyber-attacks: growing threat

Hacktivism (hacking for political, social and ideological purposes) and state-sponsored cyber-attacks are on the rise. These attacks can range from targeting government agencies to disrupting critical infrastructure. The attacks are often complex and layered, using tactics such as ransomware. With a remarkable 435% increase in ransomware by 2020, it is clear that this type of attack poses a growing threat to political targets and businesses alike.

Working from home and hybrid models: new challenges

The shift to working from home and hybrid work models has changed the way businesses operate. Collaboration tools such as Microsoft Teams and Slack have become indispensable but bring new challenges to security. One study showed that a large company can send hundreds of millions of messages annually through these platforms, often sharing sensitive information. This makes it clear that companies must not only strengthen their email security but also ensure secure collaboration environments.

As leaders, it is essential to understand that your organization's digital security requires an ongoing effort, adapted to the ever-changing landscape of cyber threats.

In the next chapter, we will delve into another form of deception that is often impossible to resist due to our human nature - *baiting*.

Checklist
TO CHAPTER 2

Train employees to recognize phishing emails

☐ **Action**: Organize monthly training sessions on recognizing phishing emails.
☐ **Action**: Send weekly samples of phishing emails for practice.

Implement email security tools

☐ **Action**: Install and configure spam filters and anti-phishing software.
☐ **Action**: Automate email security reporting to quickly detect suspicious activity.

Run phishing simulations

☐ **Action**: Use tools to conduct quarterly tests.
☐ **Action**: Analyze and discuss results during team meetings.

Ensure adequate budget for cybersecurity

☐ **Action**: Create an annual cybersecurity budget with specific allocations for phishing protection.
☐ **Action**: Conduct a cost-benefit analysis to justify the importance of cybersecurity investments.

Offer specialized training

☐ **Action**: Direct training specifically for departments such as finance and HR, given their susceptibility to attacks.
☐ **Action**: Provide advanced training for IT personnel.

Encourage a culture of reporting

☐ **Action**: Establish a simple notification system for suspicious emails.

☐ **Action**: Reward employees who report phishing attacks to promote vigilance.

Update software regularly

☐ **Action**: Schedule monthly patches and updates for all antivirus and e-mail security software.

Hacked, Now What? reveals how people—not just tech—are key to cybersecurity. With real examples and practical tips, Nathalie Claes shows how to spot risks, build a security culture, and protect your business from digital threats.

Hacked, Now What? Protect Your Business From Cybercriminals

By Nathalie Claes

Order the book from the publisher Booklocker.com

https://booklocker.com/books/14156.html?s=pdf

or from your favorite neighborhood or online bookstore.