SOCIAL ENGINEERING HANDBOOK

How to Take the Right Action

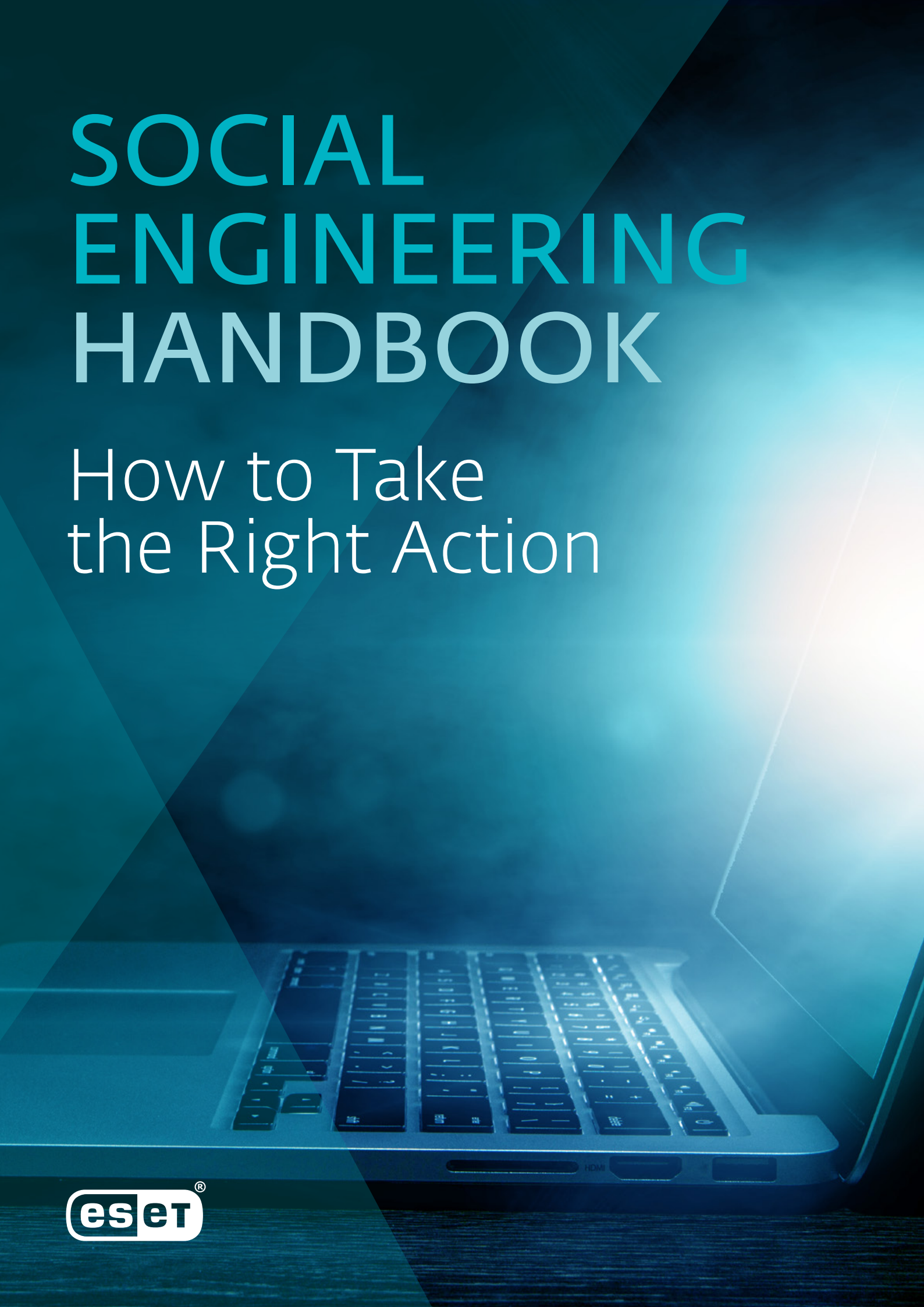


Table of Contents

Why Should SMBs Care About Social Engineering?

SMBs are increasingly aware that they are targets for cybercriminals, according to a 2019 survey conducted by Zogby Analytics on behalf of the US National Cyber Security Alliance. Almost half (44%) of companies with 251 to 500 employees said that they had experienced an official data breach within the past 12 months. The survey found that 88% of small businesses believe that they are at least a "somewhat likely" target for cybercriminals, including almost half (46%) that believe they are a "very likely" target.

The damage is real and extensive, a point well illustrated by the FBI's Internet Crime Complaint Center (IC3) annual report. In 2020 alone, the IC3 received 19,369 business email compromise (BEC)/email account compromise (EAC) complaints, with adjusted losses of over $1.8 billion. For those who don't know, BEC/EAC is a sophisticated scam targeting both businesses and individuals performing transfers of funds.

Thirty-three percent of the breaches included social attacks, the second-most-utilised tactics after hacking, states the 2019 Data Breach Investigations Report.

After SMBs experienced a breach

37%	25%	10%
suffered a financial loss	filed for bankruptcy	went out of business

Source: NCSA

Introduction

The aim of this handbook is to help introduce social engineering and its risks to every employee in the company. Humans are emotional beings, and social engineering is a very effective way to take advantage of that. What's more, social engineering attacks don't usually require highly specific technical skills on the side of the attacker. Forcing thousands of users to give up sensitive information or perform harmful actions has so far proven to be rather easy! Don't be fooled – you might easily become a target too.

On the following pages, you will find an overview of trends in social engineering, as well as examples of the most common types of attacks that can affect how employees act online. You will also learn how to recognise these attacks and protect yourself and your company.

Security solutions should protect against technical attacks. But social engineering techniques rely more on psychology – they take advantage of people's trust, fear, or inattention.

Types of Social Engineering Techniques

Spear phishing
A targeted form of phishing aimed at a specific individual, organisation, or business. Typical phishing campaigns don't target victims individually – they are sent to hundreds of thousands of recipients.

Vishing
A method that is similar to phishing, but uses fraudulent phone calls instead of emails. The cybercriminals often disguise themselves as bank or insurance company representatives.

Smishing
A social engineering attempt via SMS text messages. Most often, the smishing attempt aims to redirect recipients to a website where their data is harvested. However, there are also campaigns in which the victims are asked to send sensitive data in a direct SMS reply.

(S)extortion
(S)extortion is a long-running email scam scheme, trying to blackmail victims using baseless claims and accusations.

Impersonation
The technique of impersonation is the same as in the physical world. Cybercriminals contact employees, typically posing as their CEO, trying to manipulate victims into taking action – ordering and approving fraudulent transactions, for example.

Scareware
Software that uses various anxiety-inducing techniques to force victims into installing further malicious code on their devices. For example, a fake antivirus product tricks users into installing specific software to remove the problem, but this program is usually harmful.

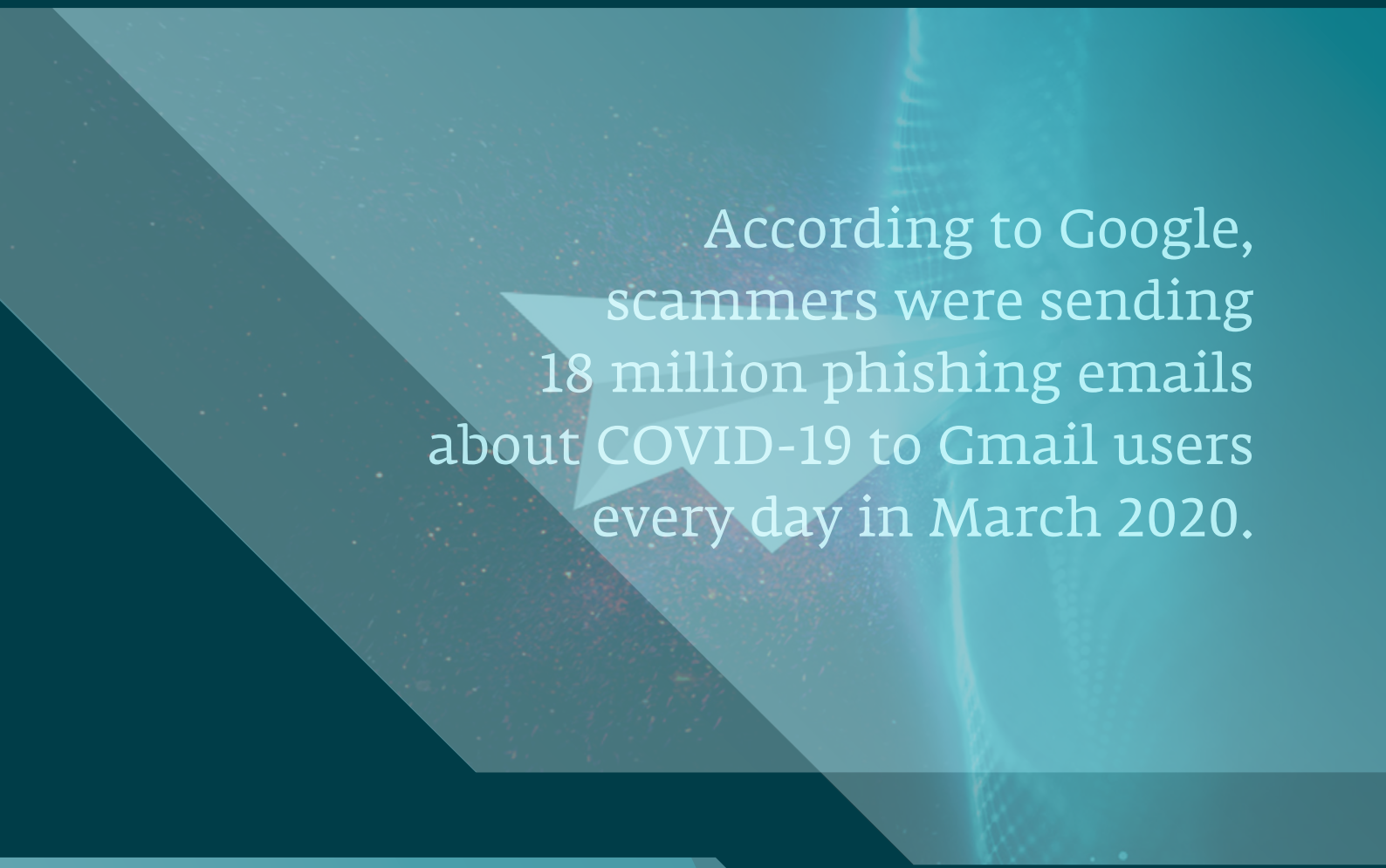
Technical Support Scams
Attackers try to sell fake services, remove non-existent problems, or install a remote access solution into victims' devices and gain unauthorised access to their data.

Phishing

You have probably already, at some point in your life, encountered a situation in which you received an email seemingly coming from a bank or some popular online service, requesting that you confirm your credentials or credit card number. This is a common phishing technique. However, phishing traps are constantly changing – and they're sometimes hard to recognise.

Phishing is a form of social engineering attack in which the attacker tries to gain access to login credentials, get confidential information, or deliver malware. Phishing campaigns can target large numbers of anonymous users, a specific victim, or a small group of associated victims with personalised scams (spear phishing). Attacks focused on specific, mostly high-profile business individuals – such as top managers or owners – are labelled as "whaling" (the bad guys going after 'the big fish').

Scammers know that there's a good chance that any message will be scanned for malicious content by your email provider, which diverts such emails to a junk folder. That's why the content of fraudulent messages changes so often.



Phishing

Since the COVID-19 pandemic started to unfold, fraudsters have wasted no time in trying to profit from the uncertainty, fear, and supply shortages connected to the crisis. In March 2020, there was a flood of COVID-19-themed spam, spreading malware, phishing for sensitive information or offering bogus products, as revealed in the Q1-2020 ESET Threat Report.

It is no surprise that the pandemic has become one of the top lures used by attackers. The appearance of any crisis brings new circumstances that provide an ideal environment for cybercriminals to innovate.

Ninety-four percent of malware is delivered via email.

$17,700 is lost every minute due to phishing attacks.

About 14.5 billion spam emails are sent every day.

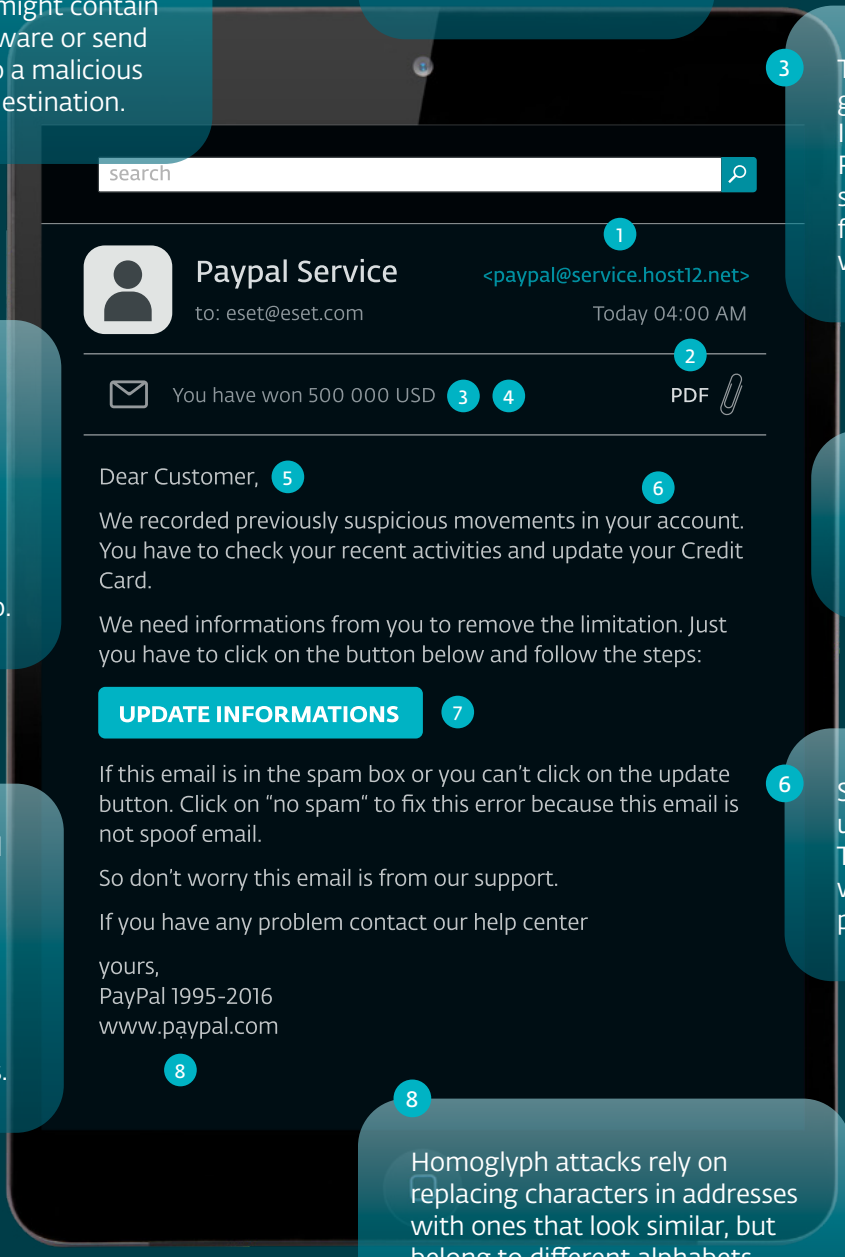
Sources: CSO, hostingtribunal.com

Basic Attributes of Phishing

1 If you are not familiar with the email address, handle the contents with caution.

2 Expect the worst from attached files or unfamiliar links. They might contain a malware or send you to a malicious web destination.

3 Too scary or too good to be true? It's probably a scam. Remember that social engineering focuses on human weaknesses.



4 The subject differs from the message.

5 If the salutation is too general, it might be a sign that it was not addressed only to you, but a number of other people too.

6 Suspicious urgency? The scammer wants you to panic.

7 Bad spelling and other grammar mistakes are common in phishing mails that have been translated from other languages.

8 Homoglyph attacks rely on replacing characters in addresses with ones that look similar, but belong to different alphabets (like "ạ" vs "a" in paypal.com).

Smishing

Smishing is a type of phishing that utilises text messaging service, or SMS. This method also spread during the first months of the COVID-19 pandemic. In confusing times, for example, people began to receive SMS messages pretending to be official messages from their local governments.

The aim of these attacks is similar to phishing – cybercriminals might **try to get personal details from you or force you to click on a link to a malicious website**. Another technique is based on our compassion. Cybercriminals send text messages with a donation request for people in desperate situations, such as a fund for hurricane disaster victims or another kind of charity, usually by asking for your credit card information.

In the beginning, it was a surprise to many people that hackers could get their phone numbers without their knowledge. But as many cybersecurity experts have pointed out, **it's easier to get someone's phone number than their email, because there is a finite number of options with phone numbers**. Guessing the names of email addresses is more difficult because they allow more characters.

Can you tell what is suspicious about this SMS?

A bank would probably never send you a direct link like this. If you are not sure, you can go to your online banking and check if you received the same message there. It's always safer to go to an official website rather than clicking on a suspicious link.

Vishing

Vishing requires even greater acting skills than other types of scams. It usually goes like this: a scammer calls you on the phone and **pretends to be a representative of an official institution**. They inform you about a compromised bank account or an unsolicited loan offer, in an attempt to get your personal information and financial details. Too good or too bad to be true? Ask them for more details, and **don't share any sensitive data immediately**. Alternatively, you can end the call and contact your bank's customer service yourself, explaining the situation.

Impersonation: When an Attacker is Posing as the CEO

Let's take a look at impersonation, another non-technical attack method used by cybercriminals to pose as trustworthy people while trying to manipulate others. How can you recognise when you are contacted by a cybercriminal instead of your colleague?

Impersonation is defined as the 'practice of pretending to be someone else' – in this case, **to obtain information or access to a person, company or computer system**. To achieve these goals, cybercriminals use phone calls, emails or messaging applications, among other methods. In many cases, attackers choose names from the company's top management and set up an email that looks as if it were written by a manager.

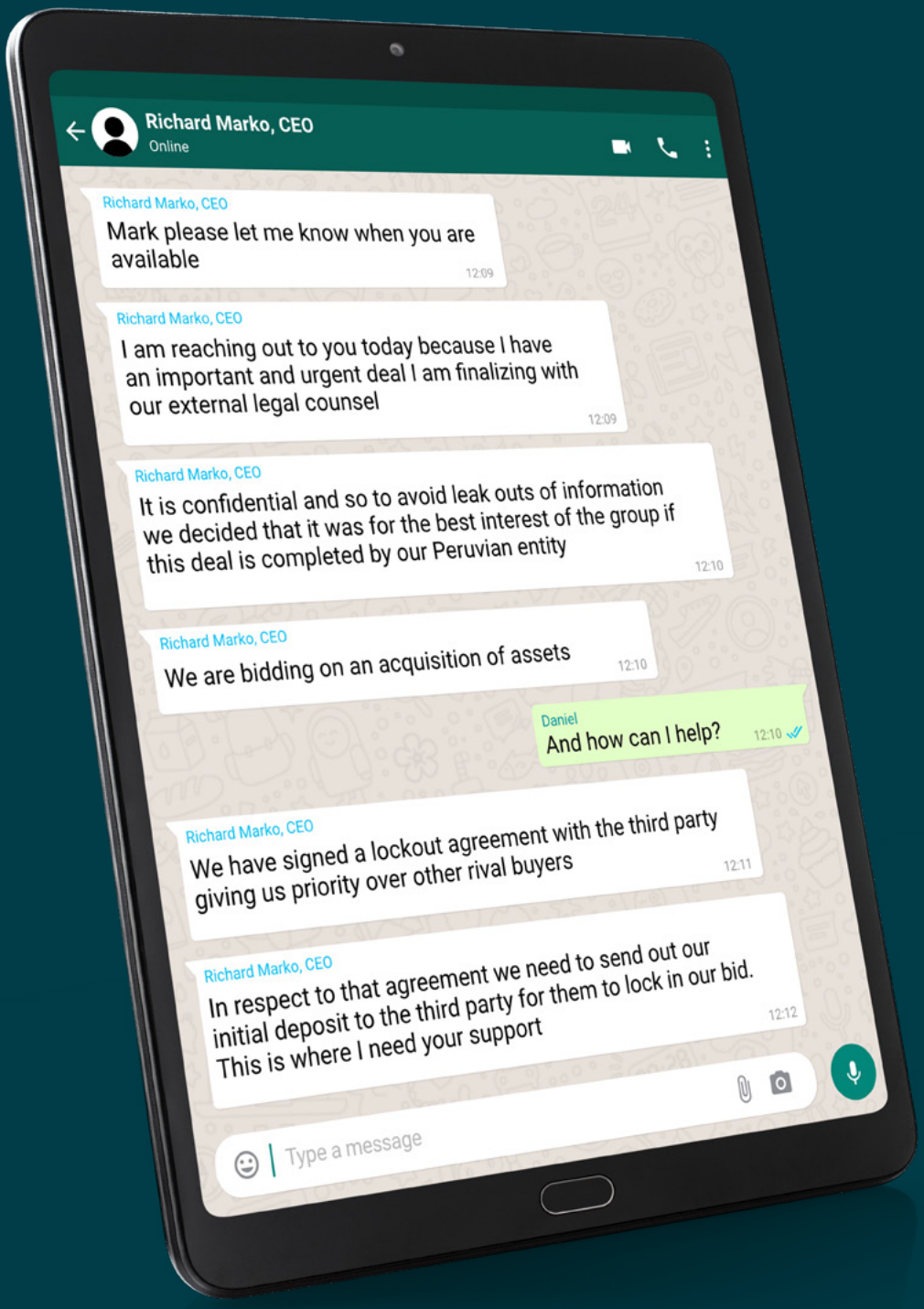
It is quite unbelievable how much corporate information is available on platforms like LinkedIn that disclose the company's structure and the names of its employees. An attacker can use such data to try to contact several employees from the company, **asking them to carry out money transfers, pay invoices, or send important data**. That's why impersonation can be so dangerous for companies – these attacks could cause a significant data breach and financial loss.

Impersonation attacks across the world rose by almost 70% in 2019, targeting businesses of all sizes.

Source: TEISS

Real Story: Impersonation Attack Against ESET

Cyberattacks can happen to any organisation. In 2020, ESET faced CEO impersonation attempts via WhatsApp messages. The goal of these attempts was to fake the existence of a big bid that required a financial deposit.



How to Deflect Impersonation Attacks

Remember, awareness is the key. The more we know about impersonation attacks, the more easily we can avoid them. Let's look at how impersonation emails work. Many try to instill a sense of urgency and fear in their targets, and that feeling leads victims to perform the desired task. This could involve something that you find unusual and suspicious, such as purchases that aren't related to your business with clients you don't recognise. Cybercriminals also try to impose a short deadline for the required tasks.

Fraudulent messages often contain grammatical mistakes or incorrect applications of corporate branding. However, those are just the easier ones to spot. Attackers adept at advanced impersonation might manufacture an email message that looks very real, including an official employee photo or signature at the end of an email. So, even if the template seems legit, be cautious if you find the request in the message odd.

THINK ABOUT THE CONTEXT

Sometimes we are too busy or rushed, and we make decisions without enough thought. Maybe it takes a few extra seconds, but always consider whether the email makes sense. Why, exactly, is this colleague asking just for this purchase or this piece of sensitive personal information? **Anything unusual and deviating from traditional processes should be a warning sign**. Even if the email apparently comes from a trustworthy person such as the CEO, it could be fraud. Stay vigilant, and verify any requests with other colleagues.

OUT OF THE OFFICE?

Sometimes, cybercriminals may know that someone is out of the office and act like they are covering for them. In that case, verify the information in question with their superior or co-workers. As the saying goes, you should look before you leap.

CHECK THE EMAIL ADDRESS

Receiving a business email from a personal account? The email address could seemingly belong to someone you know, but it is always better to answer that person at their official email address. Also, hackers sometime use an email that looks almost like an official corporate address with only a tiny deviation, e.g. replacing "m" with "rn."

Implement "EXTERNAL" tag

In a recent change by ESET internal security, emails coming from outside the company domain are always tagged EXTERNAL. This would not help if the CEO impostor was pretending to send the email from the CEO's private email, but it could help identify emails trying to fake the domain (such as the "m" and "rn" case).

VERIFY THE PERSON THROUGH ANOTHER COMMUNICATION CHANNEL

If you have received a suspicious message on WhatsApp, you should write to the person via a corporate email or call them back. Alternatively, you could simply **ask the person directly, face to face**. Don't worry about bothering someone, even when they might be busy. For example, you might be reluctant to disturb your CEO. That's natural, because the higher a colleague's position, the more hesitant we are to reach out to them, especially when they are out of the office. In that case, **consider consulting another colleague or superior**. For example, a large, urgent overdue invoice payment surely would (or should) be known to your CFO or COO, so check with them. Remember – vigilance pays off.

"Hello, my friend. You don't know me, but I know you very well. Better than you'd expect. This is your password, right?"

Emails like this can appear in anybody's mailbox. The mysterious blackmailer usually claims to have stalked the recipient via their webcam while they were watching some 'adult content', forcing the addressee to pay their way out of trouble, or else the hacker will tell their family and co-workers (sextortion). To prove that they've really hacked into the PC, they provide some password the victim uses. But (s)extortion scams are mostly swindles.

NOW IS THE GOLDEN AGE OF (S)EXTORTION SCAMS

A shining example of how hackers misuse technology and a crisis to spread scams is the COVID-19 pandemic. As many companies shifted toward remote work and home offices, where employees were not protected by the corporate network, the number of web threats increased. Cybercriminals, for example, threatened to infect the victim and their family with coronavirus for non-compliance.

By paying the demanded sum, you only lose money and fuel the business of criminals, helping them to spread more scams.

UNDERSTAND WHAT THE ATTACKER WANTS

You should know that the main purpose of (s)extortion emails is to make you pay – preferably in Bitcoins, which allows the hackers to collect the money anonymously. Scams are a great business: According to the FBI's Internet Crime Complaint Center, in 2020, (s)extortion by email caused losses of around $70.9 million.

KNOW HOW TO REACT TO (S)EXTORTION SCAMS

Do not send any money, nor reply or click on any links or attachments. If you fall victim to a (s)extortion scam, always inform company IT or internal security departments. And, if possible in your country, the incident should be reported (for example, in the United Kingdom, you can report it online to Action Fraud, and in the US, you can file a complaint on the FBI website).

The best prevention is to create a strong password or passphrase. Also, the password-selling business is another reason everyone needs to change their password regularly, and should use additional protective factors (multi-factor authentication).

IF THE PASSWORD IS RIGHT, DON'T PANIC

Mentioning a real password is just another technique to make the recipient feel nervous. The attackers may know your password, but that's probably all they have. They have probably bought the password on the dark web, or it may have been leaked in a data breach.

DON'T UNDERESTIMATE THE SECURITY CHALLENGES OF REMOTE WORK

Flexible workplaces and offices are great, but only if they are well secured and you know how to deal with them. Wi-Fi networks are highly attack-prone, so if you want to be sure that the connection and company data stays safe, you should use a virtual private network (VPN) where possible, which allows you to create a secure connection to the company network.

How do hackers get into your computer and your webcam?

If handled carefully, (s)extortion scams won't do any harm. But still, you should know that there is a way hackers can gain access to your webcam. They often use malware, for example a Trojan (horse), to infect your device with remote desktop software – but they need your assistance. Sometimes it is enough for you to simply download some unknown software. While you think you just got what you wanted, there may be some malware hidden in the file. Unknowingly, you've just helped the hackers infect your device. And don't expect the webcam light to turn on as soon as they start stalking you. Then they wouldn't be incognito, would they?

If your computer is infected, the hacker can not only see the intimate moments of your life, but they can also capture confidential data and documents, or record your discussions if they've also hacked your microphone.

How To React to a (S)extortion Message

1. Act carefully and deliberately, and avoid rash actions.
Criminals behind (s)extortion scams target human weaknesses and try to manipulate you into harmful action. Therefore, if you receive a fear-inducing message, stop and consider the possibility that nothing in the email is true. If you are unsure, always consult the IT department or tech support of the security provider.

2. Don't pay the (s)extortionists.
(S)extortion emails are usually just scams. This means there is no merit behind the claims of the criminals; they almost certainly have no video of you or what you watched, they are not with law enforcement, and they didn't order a hit on you.

3. Do not interact with the email in any way.
Do not reply to the scam, do not download its attachments and do not click on embedded links or interact with any of the contents, as these elements can lead to malware or other threats.

4. Check/change your password.
In some cases, criminals test the leaked credentials and, if successful, use the hacked account to spread their messages. Therefore, if an attacker lists any of your actual passwords, change them immediately and activate multi-factor authentication to increase your accounts' protection.

5. Send the email to your IT department.
If your company has no IT staff, the least you can do is to scan the computer and network with a reliable security solution and make sure that none of your passwords have been leaked or compromised.

6. Secure your webcam.
To avoid possible misuse of the built-in webcam, use protective software or at least put a piece of tape over the camera. This way, you can be certain that criminals have no way to record a video of you sitting in front of the device.

7. Use an anti-spam solution.
A reliable security solution with anti-spam functionality can help stop (s)extortion scams from landing in your inbox in the future.

Other Types of Social Engineering Techniques You Should Know About

Scareware is a type of malware that tries to trick victims into purchasing and downloading potentially dangerous software. It is a method that very quickly attracts people's attention and... scares them. Pop-up ads that are difficult to close, software companies with names you have never heard of and unauthorised scanning of your computer for viruses – all of these are typical attributes of scareware.

The problem is that such programs usually proceed to display a list of dozens or hundreds of fake viruses. But scareware programs are not scanning your computer, and these claimed-to-be-uncovered results are fake. Warnings about an infection only manipulate you into actually downloading one. These scams often rely on fake security software, such as Advanced Cleaner, SpyWiper, or System Defender.

Stick with known, tested, and up-to-date software products

Thus, you will know that an invite to download free software might be a scam. It is also very useful to use pop-up blockers on your work devices and URL filters. Establish web security tools and firewalls to stop attackers in their tracks.

Technical support scams are closely related to scareware. But unlike scareware, they pretend to come from an established company such as Microsoft. They won't automatically start scanning your computer. Instead, they may ask you to open some files – and then tell you those files show a problem that doesn't exist. According to the US Federal Trade Comission (FTC), tech support scams are not uncommon. In 2019, the FTC received more than 100,000 reports of such scams.

Checklist for IT Admins:
Five Ways to Protect Your Organisation from Social Engineering Attacks

1. Regular cybersecurity training of all employees, including top management and IT personnel. Remember that such training should show or simulate real-life scenarios. Learning points must be actionable and, most of all, actively tested outside the training room.

2. Scan for weak passwords that could potentially become an open door in your organisation's network for attackers. Additionally, protect passwords with another layer of security by implementing multi-factor authentication.

3. Implement technical solutions to tackle scam communications so that spam and phishing messages are detected, quarantined, neutralised, and deleted. Security solutions, including many that ESET provides, have some or all of these capabilities.

4. Create understandable security policies that employees can use and that help them to identify what steps they need to take when they encounter social engineering.

5. Use a security solution and administrative tools, such as ESET PROTECT Console, to protect your organisation's endpoints and networks by giving administrators full visibility and the ability to detect and mitigate potential threats in the network.

For over 30 years, ESET® has been developing industry-leading security software for businesses and consumers worldwide. With security solutions ranging from endpoint and mobile defence to encryption and two-factor authentication, ESET's high-performing, easy-to-use products give users and businesses the peace of mind to enjoy the full potential of their technology. ESET unobtrusively protects and monitors 24/7, updating defences in real time to keep users safe and businesses running uninterrupted. For more information, visit www.eset.com/uk.