FROM CRISIS RESPONSE TO TRANSFORMATION

THE ROLE OF DIGITALIZATION IN THE COVID-19 PANDEMIC AND IN THE FUTURE

The COVID-19 pandemic has shown the importance of having a thought-through remote workplace strategy in place. We decided to share our experience with the switch to working from home, predict what role flexible workplaces will play in the future and provide advice on how to create them. This handbook can provide inspiration for CISOs, CIOs and IT managers as well as enlightened CEOs who want to discover the magic of digitalization.

May 2020

CONTENTS

PART 1

ESET CASE STUDY:

How we made it through the COVID-19 pandemic and what we've learned from it

The COVID-19 pandemic has been a new experience for humankind. So it has also been new for ESET–we had prepared several crisis plans in the past, but none of them could reflect all of the challenges that the pandemic has brought. From the very beginning of the crisis, two things were essential: to keep our employees safe and to work remotely in order to keep the business running. Here's how we managed.

PART 1

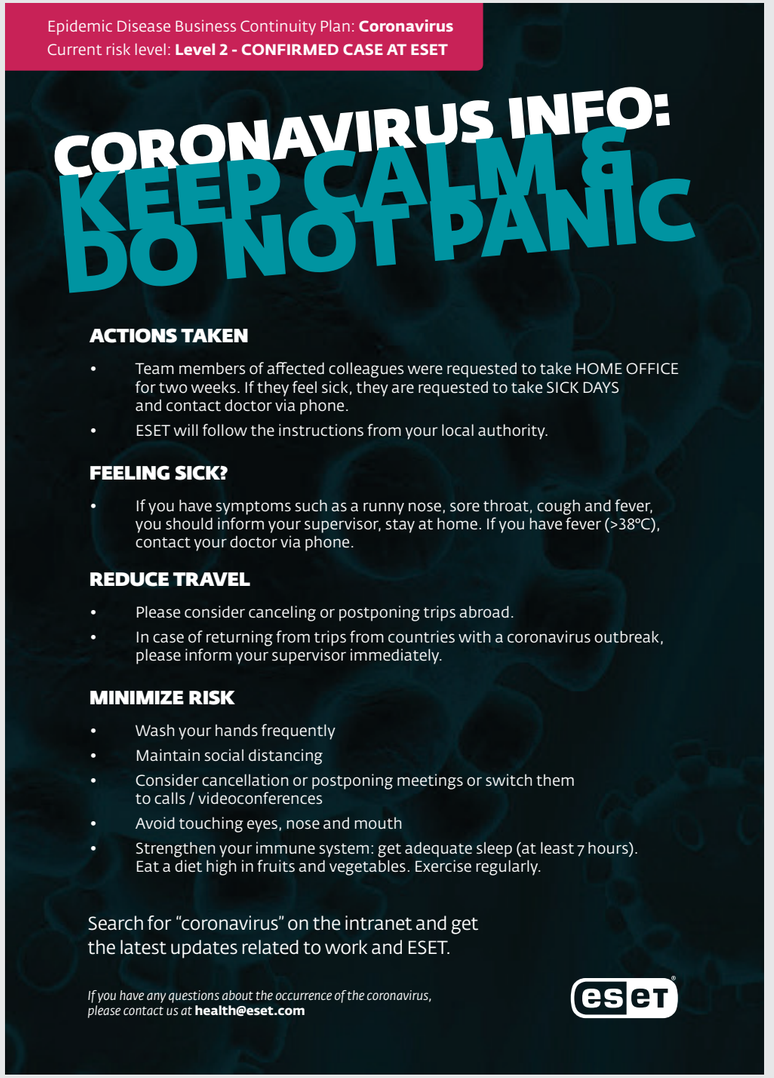
INFORMATION IN THE FIRST PLACE

Lack of information causes trouble–in the beginning, many of our employees panicked. As soon as we knew the situation was getting serious, we set up a special email address to which our employees could anonymously send questions.

Also, our employees were very active in trying to find information about COVID-19. We saw several cases when they were consulting untrustworthy sources and downloading files that could potentially harm their computers. Therefore, we provided them with a list of reliable media and expert sources, recommending, e.g., the studies conducted by the World Health Organization (WHO) or Johns Hopkins University (JHU). Furthermore, we shared some tips on how to be productive while working from home and advised managers on how to manage their teams remotely.

Since some of our employees do not possess company devices, we also produced simple posters with all kinds of relevant information–from how to wash your hands to which online tools to use and how to reach out for help. This was just one of the few offline measures we implemented.

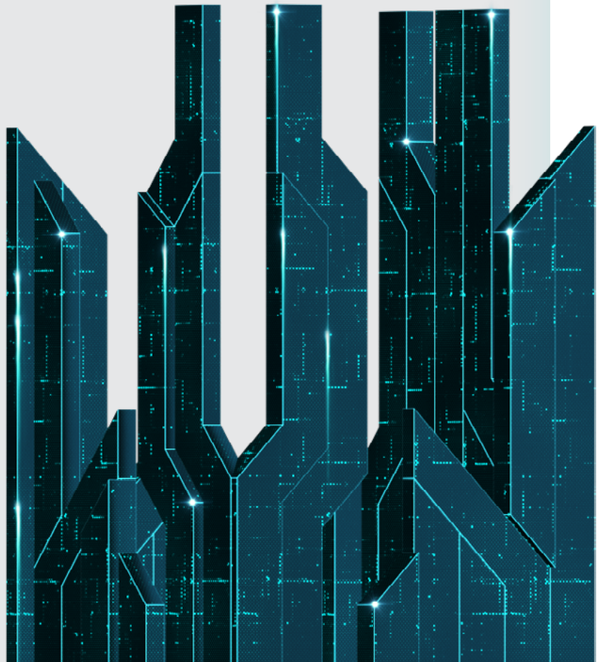
POSTERS FOR EMPLOYEES, WITH PANDEMIC MEASURES AND RECOMMENDATIONS



PART 1

PLANNING, PLANNING AND PLANNING AGAIN

The situation was gradually escalating around the globe, so we were updating our pandemic flu business continuity plan accordingly. We had some backup plans from the past, like the one from the gas crisis of 2009, but those were outdated. In our new crisis plan, we took three different stages into account.



LEVEL 1: MONITORING

The first stage applied when the pandemic was already present in some of the countries where ESET offices operate. At this point, we were also looking for ways to protect colleagues on or scheduled for business trips, creating, e.g., a blacklist of risky countries. For conferences organized by ESET, we also created a list of alternative programs that could immediately replace the speech of a sick speaker–including longer coffee breaks, ESET quizzes or panel discussions.

LEVEL 2: LIMITED OFFICE USE

The next phase reflected the moment when we anticipated that there could be an infected employee or when the government might come up with regulations that could affect multiple teams. We also started to offer organized webinars with psychologists. Our HR department played a crucial role at this point.

LEVEL 3: OFFICE CLOSURE

The final stage took into account that there might be a forced quarantine, or that the management might decide that the whole company should work remotely, which is what actually happened.

PART 1
PLANNING, PLANNING AND PLANNING AGAIN

In the beginning of the crisis, we also established a Health Committee, consisting of five individuals: ESET's Business Continuity Manager, Chief HR Officer, our Chief Operating Officer, as well as both the IT Support Manager and Facilities Manager. Their responsibility was to monitor the situation on a regular basis, next steps and communications, perform risk assessments and help C-level management make important decisions. As for our international offices, we recommended to whom HR and Country Managers, as well as regional directors, should discuss the impacts of these decisions with, and alerted them that they were obliged to report back to the Health Committee.

We also had to set rules for travel to other countries. As soon as we reached Level 2, we complied with the recommendations of the Ministry of Foreign Affairs of the Slovak Republic and advised our employees not to travel anywhere.

THIS IS HOW CISO, DANIEL CHROMEK ORGANIZED OUR PANDEMIC FLU BUSINESS CONTINUITY PLAN AND SUPPORTED CROSS-DEPARTMENTAL COMMUNICATIONS.

ROLE	RESPONSIBILITY
HEALTH COMMITTEE 1. Business Continuity Manager, 2. Chief HR Officer, 3. Chief Operating Officer, 4. IT Support Manager and 5. Facilities Manager	Planning response, preparation of communication, monitoring situation, preparation of information necessary for C-level management decisions.
HR MANAGER IN ESET OFFICE	Communication to employees. Handling the outbreak within the ESET office. Reporting back to health committee.
COUNTRY MANAGER IN ESET OFFICE	Decisions on office in position of C-level management. Decides on office closure and approving additional costs together with: • regional director and Chief Business Officer / Chief Sales Officer (whoever reached) for S&M Offices • Chief Technology Officer or Chief Software Architect for R&D offices
REGIONAL DIRECTOR FOR EMEA, APAC, NORAM AND LATAM	Decides on office closure together with country manager. Approving additional costs.

PART 1

EVEN TECH COMPANIES CAN HAVE PROBLEMS WITH TECHNOLOGY

You might think tech companies can't get stuck when transitioning to remote work... since they are the experts in IT. While we did not face any troubles regarding security, we did experience organizational problems.

As soon as it was clear that all employees would have to work remotely, we had to get additional laptops for a number of employees who had been working on desktop PCs after discovering that in fact we did not have enough of them on hand. Therefore, our IT team had to visit several warehouses and shops to get everything we needed–that held us back in the beginning. In the end, some of our employees had to take home whole desktops and other accessories. Next, all the new devices had to be set up very quickly–eventually, our IT specialists managed this effort in three days, during a long weekend shift. Lesson learned: always check whether or not you have the required technical equipment to work from home.

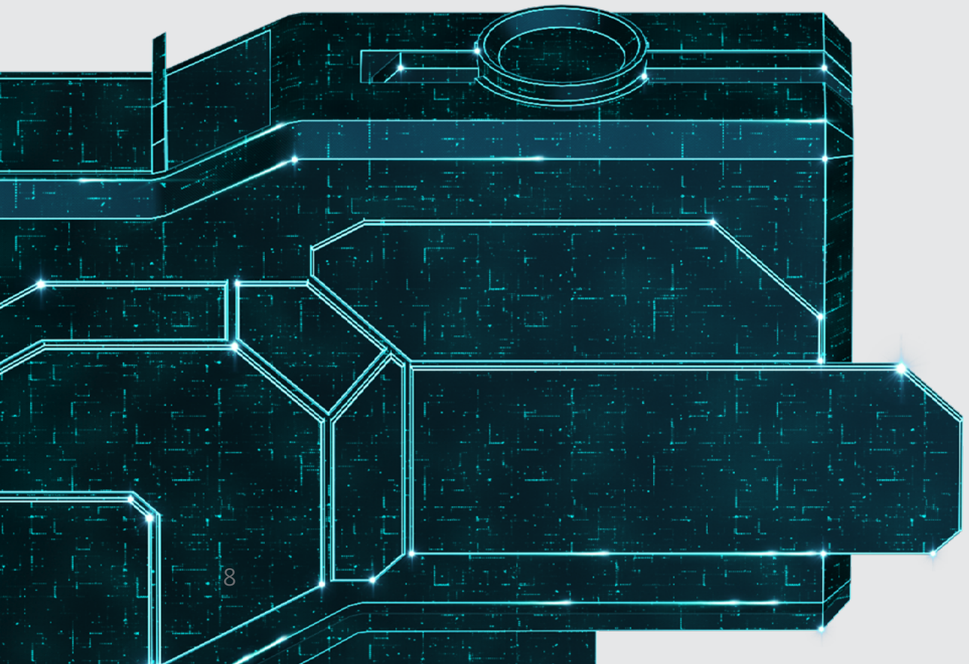
With that solved, it also turned out we lacked enough VPN licenses to enable all our employees to connect to internal systems from home. Unfortunately, our vendors had trouble covering the demand, and we had to wait longer for them to deliver the services we needed. This clearly showed that even if you try hard to create the best crisis plan, it can all fail due to a supplier's lack of services on which your company is dependent.

Daniel Chromek, ESET CISO

"Suddenly, the situation escalated very quickly, and 80% of our employees needed remote access... All of the desktop hard disks had to be encrypted, and new laptops needed to be prepared very fast, which was pretty demanding.

PART 1
SECURITY FIRST

Outside of the corporate network, devices are more vulnerable to cyberattacks. In order for us to be able to keep both the devices and all the data safe, we focused on vital additional security layers for endpoint protection and mail security–from full disk encryption and multifactor authentication to cloud sandbox technology.



ESET SOLUTIONS WE USED DURING THE CRISIS

ESET Endpoint Security 7: Endpoint protection platform that combines strong malware, exploit and ransomware prevention, augmented by machine learning.

ESET Dynamic Threat Defense: Cloud sandbox leveraging multiple machine learning models to detect and analyze threats on endpoints and in email attachments; and detects both zero-day and ransomware threats.

ESET Security Management Center: Management console that controls endpoint prevention, detection & response layers across all platforms–desktops, servers, agentless virtual machines and managed mobile devices via a single pane of glass.

ESET Secure Authentication: A simple yet powerful way to implement multifactor authentication designed to work on all phones, HW tokens, all VPNs and cloud services, with a push authentication feature that is extremely easy to use.

ESET Full Disk Encryption: A powerful encryption managed natively by ESET remote management consoles, increasing organizations' data security to meet compliance regulations.

READ MORE ON HOW TO SECURE YOUR REMOTE WORKFORCE.

PART 1

THE CRISIS AS A CATALYST

Despite causing a lot of trouble, the crisis made us focus on new processes and solutions, which we are confident will help us in the future. We finally started using electronic signatures, reached maturity in our online hiring processes and boosted our remote administration capabilities. Not only did we learn how to work remotely without having to cancel a single important project, but also how to be more productive. That is something that will certainly help us in the long term.

Even before the crisis, we knew that our employees longed for more flexibility–and the crisis helped us meet their needs. We believe that a fully digitized workplace is the future, and thanks to the pandemic, we took several steps towards it.

TIMELINE: OUR CRISIS RESPONSE IN TIME

JANUARY

NUMBER OF MALWARE FILES REPORTED AND DELETED FROM OUTLOOK: 6

FEBRUARY 1st

LEVEL 1: MONITORING–NUMBER OF PEOPLE IN THE SLOVAK OFFICES: 800

FEBRUARY 4th

SETTING UP A SPECIAL E-MAIL DESK

MARCH 10th

ESTABLISHING THE HEALTH COMMITTEE

MARCH 12th

LEVEL 2–LIMITATION OF OFFICE USE

MARCH 15th

LEVEL 3–OFFICE CLOSURE

MARCH 16th

PROCURING ALL REMAINING NECESSARY DEVICES

MARCH 18th

SUCCESSFULLY SETTING UP ALL NEW DEVICES

APRIL

NUMBER OF MALWARE FILES REPORTED AND DELETED FROM OUTLOOK: 27

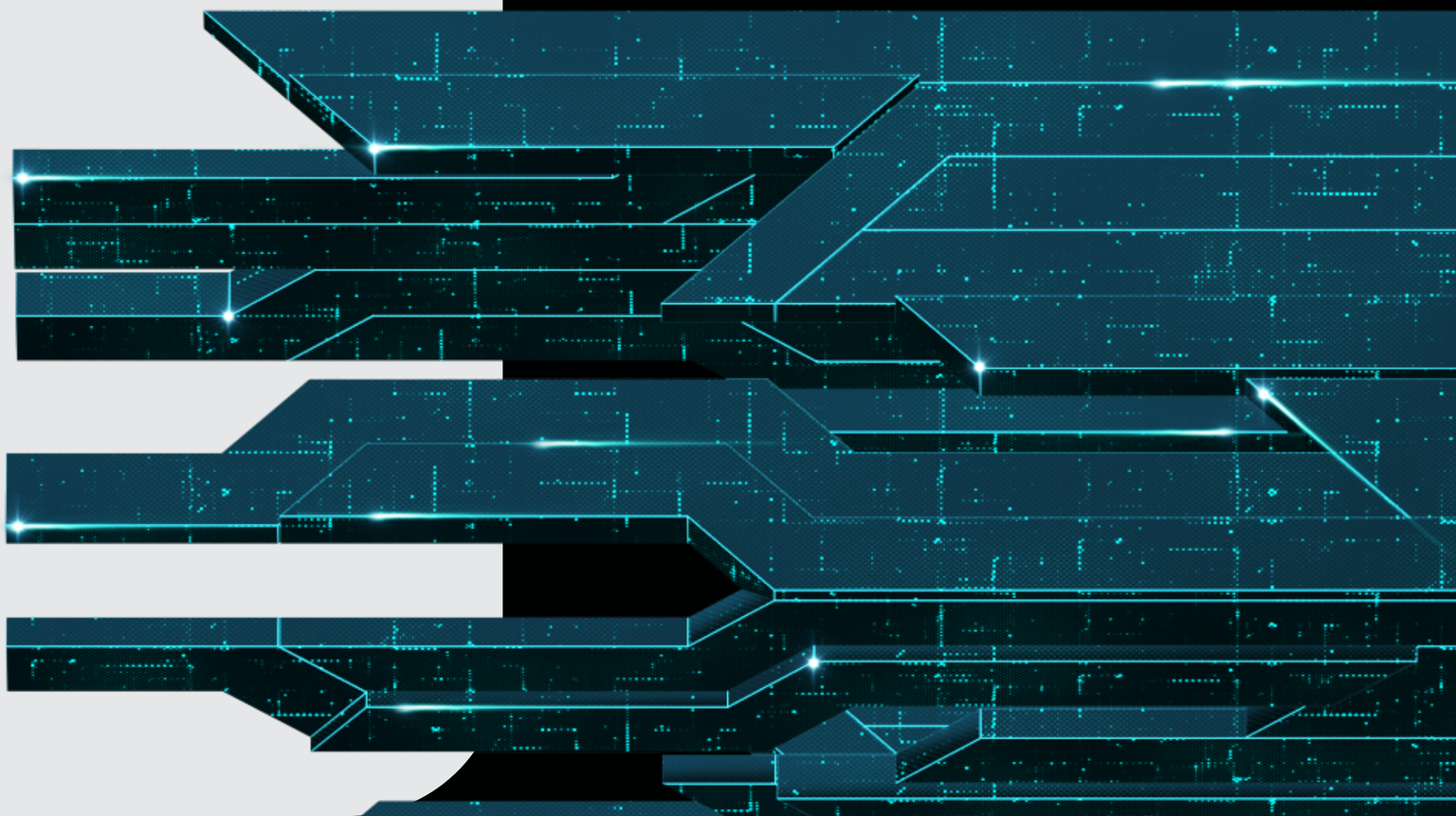
APRIL 10th

ALMOST EVERYONE WORKING REMOTELY–NUMBER OF PEOPLE IN THE SLOVAK OFFICES: 25

PART 2
NEW THREATS IN THE GAME

Ethics and morals? Nothing for cyber criminals. Crises are ideal occasions for them to start their attacks. They take advantage of employees being stressed, anxious and under pressure, and your company rushing to introduce new measures to survive. "Criminals have quickly seized opportunities to exploit this crisis by adapting their modes of operation or developing new criminal activities," says the Executive Director of Europol, Catherine de Bolle in a recently published handbook.

Our experiences have confirmed Ms. de Bolle's words. We have been receiving twice as many phishing emails as normal. Some of the senders have even been using names and contacts of real ESET employees, asking recipients to pay fraudulent invoices, perform certain tasks or share their bank account details.



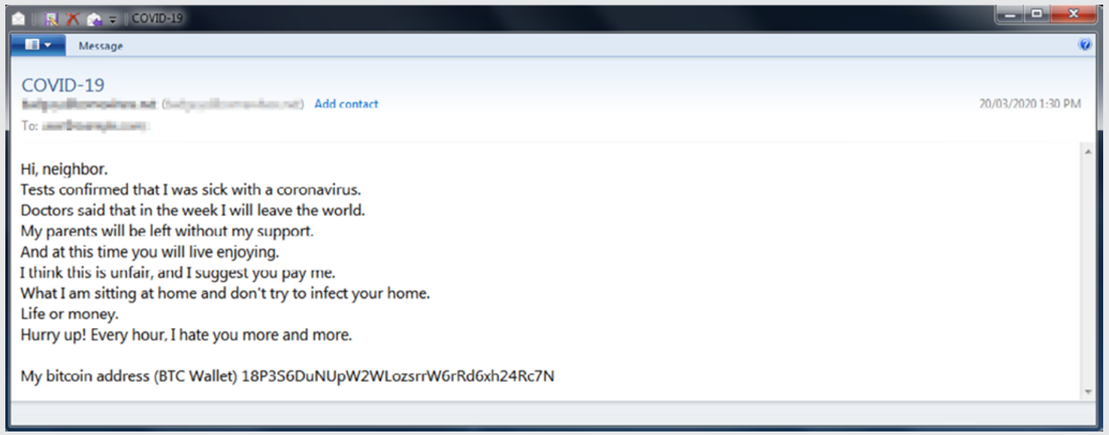
PART 2
WEB THREATS

The coronavirus topic has been used as a lure in multiple web threats. According to the ESET Threat Report Q1 2020, the number of fraudulent websites blocked in Q1 2020 increased by 21% compared with Q4 2019.

Cybercriminals, for example, have made use of the high demand for medical supplies and founded fake e- shops with such equipment. They let users pay, but they either never received the order, or got substandard goods. According to Europol, authorities around the world seized around 34,000 counterfeit surgical masks between the 3rd and 10th of March 2020 alone. With the facts on the ground developing as they were, ESET strongly further focused on staff awareness, too, regularly informing our employees about such threats and scams.

Cybercriminals even threatened to infect email recipients and their families if they refused to pay ransom. Also, so-called business email compromise (BEC) attacks increased, and companies faced even more ransomware and malware attacks.

CORONAVIRUS-THEMED EXTORTION SCAM EMAILS



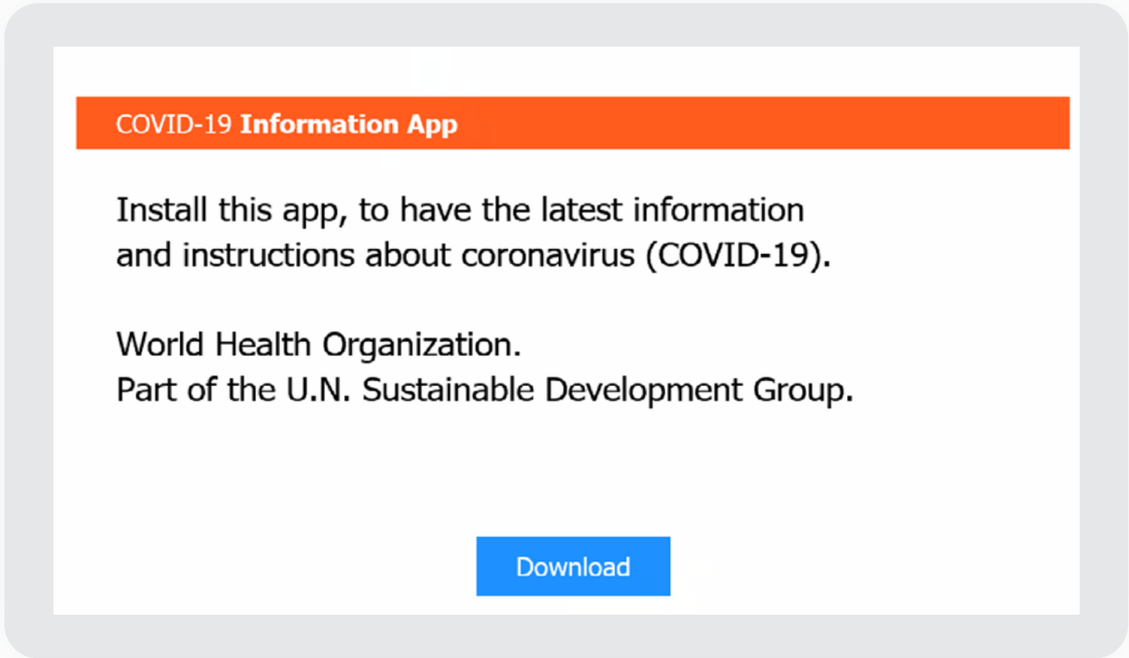
LEARN MORE ABOUT HOW SCAMS EXPLOIT CORONAVIRUS FEARS AND ABOUT DIGITAL CHALLENGES THE VIRUS HAS BROUGHT.

PART 2
FAKE AUTHORITIES

ESET employees were not the only ones benefiting from the trust placed in the WHO. Sadly, the organization was one of the most impersonated authorities being leveraged in scam campaigns, and unfortunately they became a door through which attackers were spreading fake news, pretending to have important information and asking users to click on malicious links–among other goals, the attackers set out to steal personal data.

> *The attackers take advantage of the fact that people are nervous and working from home.*
>
> **Daniel Chromek, ESET CISO**

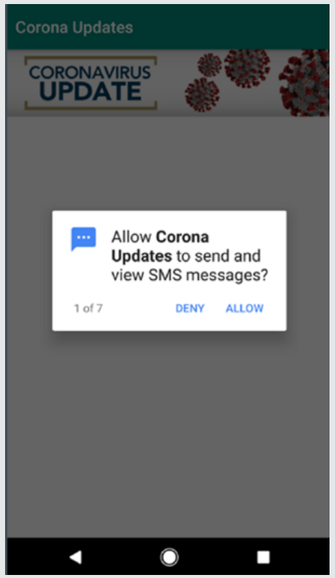
MALICIOUS WEBSITE IMPERSONATING THE WHO AND LURING USERS INTO DOWNLOADING MALWARE.

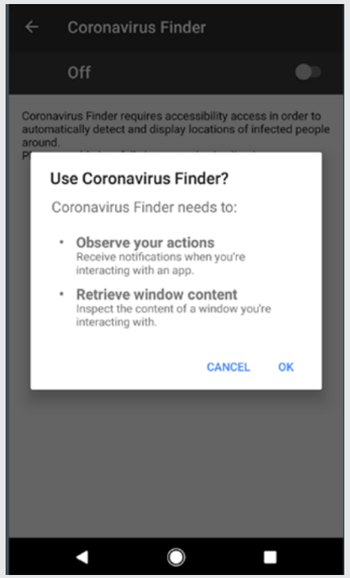


PART 2
DANGEROUS APPS

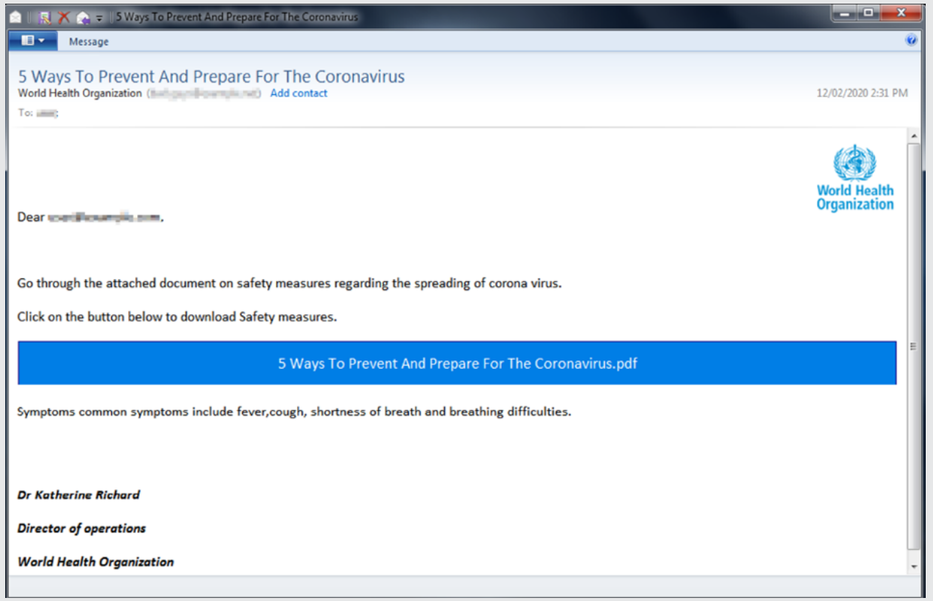
Furthermore, new malicious apps appeared promising users symptom identification, contact tracing or financial compensation. Many such apps were infected by banking Trojan families, ransomware, spyware and adware.

EXAMPLES OF CORONAVIRUS-THEMED ANDROID MALWARE PERMISSIONS REQUESTS





SPAM EMAIL IMPERSONATING THE WHO.



SOURCES OF IMAGES: ESET THREAT REPORT 2020

PART 2

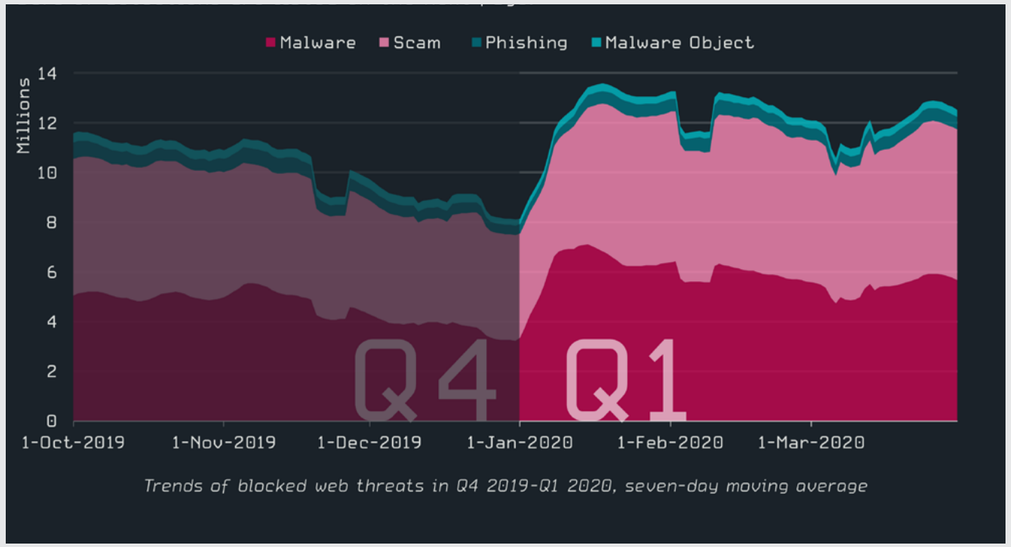
COVID-19 CYBERATTACKS IN NUMBERS

- 18 million daily malware and phishing emails related to COVID-19 were spotted by Google in the second week of April 2020. On average, Google blocks more than 100 million phishing emails a day.*
- 240 million COVID-19-related spam messages were spotted daily by Google during the COVID-19 peak.
- 600 %–is the recorded growth of covid-19 related phishing emails measured worldwide in the first quarter of 2020, according to KnowBe4 research.

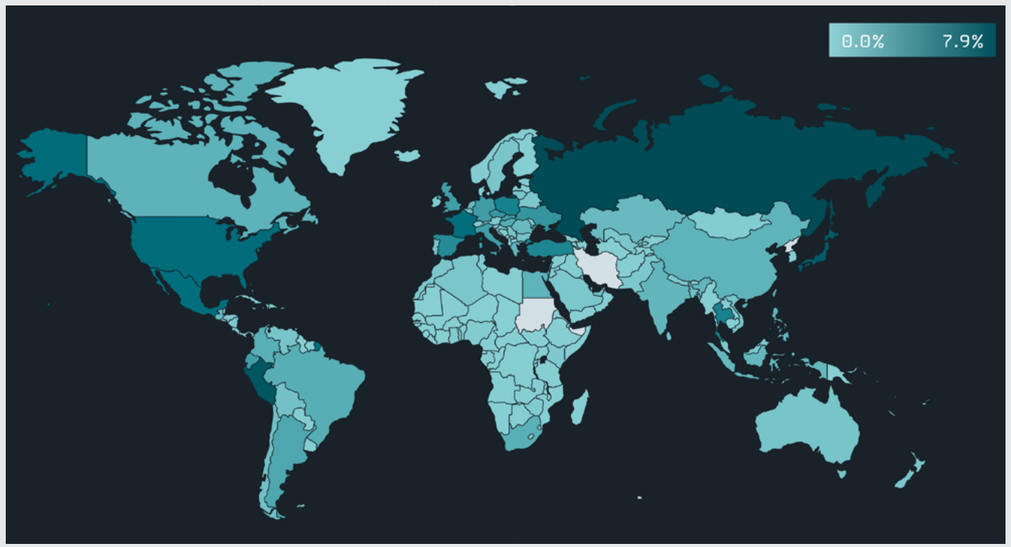
* *ESET is a founding member of the App Defense Alliance to protect the Google Play Store, providing its award-winning detection capabilities and improved security for the Android ecosystem. ESET also protects Google Chrome users, via an embedded ESET engine in Google Chrome Cleanup, a security tool that alerts Google Chrome users to potential threats; and also has an integration with Chronicle, a division of Google Cloud*

Read more about how ESET cooperates with Google.

TRENDS OF BLOCKED WEB THREATS IN Q4 2019-Q1 2020, SEVEN-DAY ROLLING AVERAGE



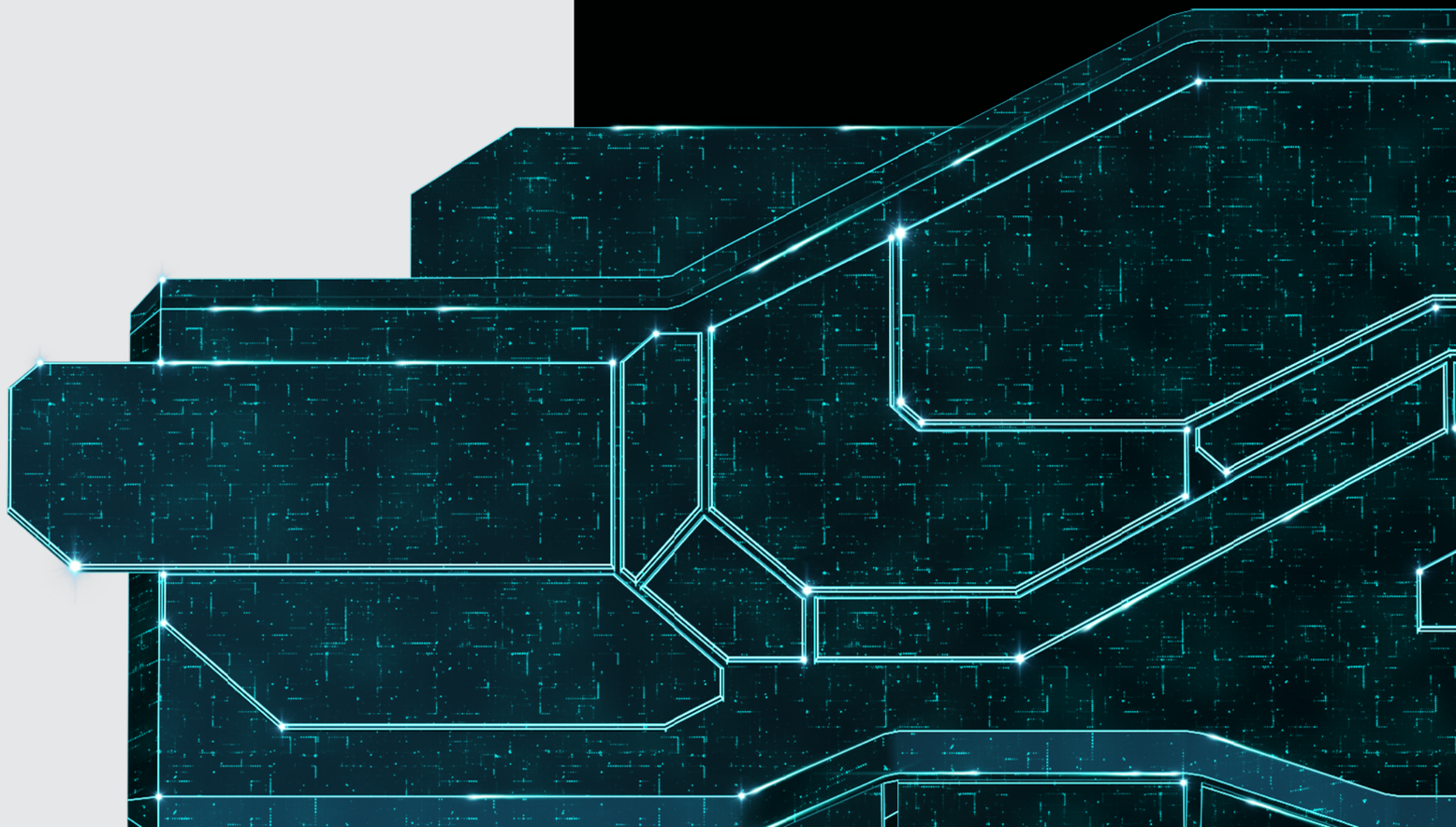
Trends of blocked web threats in Q4 2019-Q1 2020, seven-day moving average



PART 3

STAY ON TRACK: 6 TAKEAWAYS FOR THE FUTURE

Albert Einstein was right when he said that "in the midst of every crisis, there lies an opportunity." The COVID-19 crisis can serve as an initiator of a new working reality. Digital and remote workplaces are the future–and the future starts now. How should we proceed to manage safe and flexible working environments?



PART 3

1. EVALUATE HOW THE CRISIS HAS AFFECTED YOUR COMPANY

Maybe the crisis finally made you integrate new tools and processes into your daily routine and functioning. In order to be able to analyze which solutions might be helpful in the future, here are some questions to ask yourself.

QUESTIONS THAT HELP YOU DEFINE WHAT MEASURES (NOT) TO KEEP AFTER THE CRISIS

- What operations had to be cancelled due to the crisis and why?
- Compared with the situation pre-crisis, is your IT architecture now better able to fulfill the business needs of the company?
- Would the company have withstood the crisis better if more processes and operations were digitized?
- Why would it be advantageous/disadvantageous for the company to keep working remotely and pursue further digital maturity?
- Would it be convenient to further improve the new policies and processes your company adopted during the crisis?
- If so, what tools and measures support this manner of work and would also be a good investment for the future?
- How does the company's management perceive the experiences of both the crisis and digitalization?
- How do your employees perceive this mode of work?

PART 3

2. REVISE THE BUSINESS IMPACT ANALYSIS AND THE BUSINESS CONTINUITY PLAN

Planning and prioritizing are essential, not only in times of crisis. Taking the experience from the crisis into account, in cooperation with the continuity planning department, redefine which departments need to raise their digital maturity, because they sit at the core of the business.

You should now focus on projects that will allow you to work remotely. Are there projects that are crucial to the company that, until now, were not able to be transformed or transferred into the digital environment? Or were the solutions you came up with during the crisis insufficient? It's time to ensure you can deliver the same services in the same quality online.

Your company's business impact analysis and business continuity should reflect the critical nature of particular services as well as the role of IT. The crisis might have shown some plans need to be revised–share your takeaways with management.

HOW TO TALK TO YOUR BOARD ABOUT CYBERSECURITY AND BUDGETS

A. CYBERSECURITY IS THE KEY TO NEW BUSINESS OPPORTUNITIES

Digital solutions can bring new business opportunities. But also, inadequate data protection can result in huge data and revenue losses, damaging the overall trust in the company as well as its reputation. Reassuring the company's customers that their data is well-secured will raise the company's credibility.

B. PRESENT ENOUGH EVIDENCE

Bring concrete statistics on how cybercrime is rising and how even one wrong click can harm business. To prove how dangerous, e.g., phishing can be, perform a test on the company's employees: send them a few fake emails and see how many of them click on a malicious link.

Also, try to hire a white hat hacker and ask him / her to try to penetrate your company's network.

C. MAKE CYBERSECURITY FUN

Come up with ideas for how to raise cybersecurity awareness at your company by creating interactive training materials. One learns through play; data security is no exception.

PART 3

3. IF YOUR COMPANY'S NEW TO DIGITALIZATION, START WITH SMALL STEPS

If it is clear that your company has yet to take significant steps towards digitalization, the magic will not happen in one day. Regardless, even small changes matter. Create a digital workplace strategy, starting with small steps like transitioning corporate accounting towards an online- only environment. This will allow you to manage your finances from anywhere and at anytime– and if the whole company suddenly needs to work remotely, digitized accounting will already be in place.

Generally, finding solutions that will help eliminate physical contact between individuals (when necessary) is key to successful digitalization. This is also an appropriate approach to take when aiming to prevent service outages due to illness.

PART 3

4. EXAMINE THE PREPAREDNESS OF YOUR SUPPLIERS

Most companies are dependent on external suppliers and services. If they fail to deliver, you might fail to withstand the crisis. Therefore, it is crucial to know how ready they are to meet their contract obligations or even expand their offer even in times of crisis.

It helps to have multiple solutions for a single problem. If an app or service fails, there should be a backup solution, so that employees are always able to perform any task or communicate online.

QUESTIONS TO ASK YOUR SUPPLIERS AND BUSINESS PARTNERS

- Do you have a pandemic flu business continuity plan in place?
- Have you tested your pandemic flu business continuity plan in the past year?
- Is the process you deliver to our company affected by the risk of high rates of absence amongst your employees?
- If so, did you apply any measures to minimize the risk of high rates of absence amongst your employees who are delivering services to our company?
- Do you have a list of suppliers for critical processes?
- Is the process you deliver to our company affected by the risk of outages from other suppliers?
- If so, have you applied any measures to minimize the risk of outages at other suppliers that participate in deliveries to our company?
- Do you have a post-crisis resumption plan in place?
- Is your staff trained on crisis management?

PART 3

5. ADAPT SECURITY SOLUTIONS TO THE CHANGES

While moving business processes online can improve business continuity during crisis, it can also bring additional cybersecurity risks. Therefore, your role should not only be to guarantee high accessibility, but also to protect corporate and personal data accordingly. Adequate connectivity is a must, too–therefore, a virtual private network (VPN) is essential for countering the increased security risks. All remotely working employees should have a VPN license to be able to safely connect to the corporate network.

Another precondition of an effective remote and digitized workplace is having enough devices employees can use from home. But what if your company cannot afford any new laptops or tablets at the moment? Consider under what conditions employees might use their personal devices, such as laptops, smartphones, desktops and tablets. Critically, at a minimum each device will have to be secured properly with anti-malware protection that is up to date, using a fully fledged multilayered endpoint protection solution from a reliable vendor, not a free antivirus.

CYBERSECURITY STARTER PACK FOR AN EFFECTIVE DIGITIZED WORKPLACE

- automated and standardized environment for easy remote administration. Standardize not only technical tools, but also processes.
- reliable endpoint protection software, which can be used for corporate as well as personal devices
- reliable local hard disk encryption
- detailed monitoring of each app and data
- strong passwords supported by MFA and effective group policies
- create hybrid environments by combining on-premise and cloud deployments to best effect

PART 3

5. ADAPT SECURITY SOLUTIONS TO THE CHANGES

USING NEW APPS SAFELY CAN BE A CHALLENGE, LIKE THOSE FOR VIDEOCONFERENCING. HERE ARE A FEW TIPS ON HOW TO MEET-UP SAFELY.

- be sure only authorised individuals join meetings. Create user groups or restrict access by internet domain.
- set strong meeting passwords and do not embed the password in the meeting link.
- let the participants wait in the meeting room and approve connection for each one. The larger the meeting, the higher the chance an uninvited guest appears.
- encrypt video. Some services only encrypt chat!
- limit file exchange by time. Don't allow executable files to be exchanges by participants.
- choose what to share on your screen with others. You might need to share only one application, not the whole desktop.
- check your environment. Even papers on your desk might include sensitive information, giving away corporate secrets.
- check the privacy policy of the service you're using. It can be that free apps collect and sell your data to fund the provision of the service–you might become a product.

READ MORE ON HOW TO MEET ONLINE SAFELY.

READ MORE ON SECURING PERSONAL AS WELL AS CORPORATE DEVICES WHILE EMPLOYEES ARE WORKING FROM HOME.

PART 3

6. TRAIN YOUR EMPLOYEES AND EMPATHIZE WITH THEM

Even though IT is commonplace for you, not everyone is so familiar with the digital world. Organize regular cybersecurity trainings and workshops. Also, be sure employees can always reach out for help–a special email for anonymous inquiries is a good solution.

Introduce digitalization and new online tools as helpful components, not as an obligation. Words matter–speak clearly and use simple language, and if you struggle to explain or your employees fail to grasp the information, try to cooperate with your HR department or communications teams. A short excursion into the human mind might help. Keep in mind that there is no such thing as a stupid question.

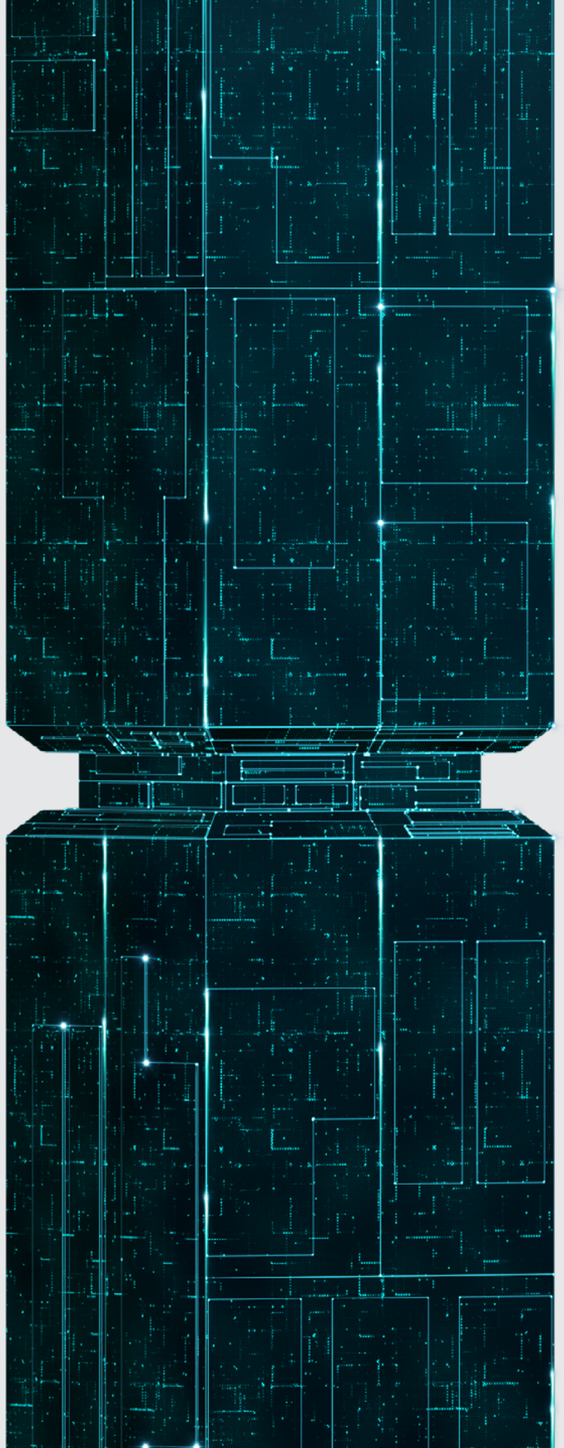
Try to evaluate employee effectivity per task, not per hour. The best stimulant is motivation: get to know your employees well and find out what kind of tasks they enjoy. Attractive tasks bring the best results and high productivity, and employees will be more open to using new digital tools. Last but not least, regularly evaluate employee feedback, and care about their opinions, problems and ideas.

Also, when stressed and working remotely, employees often read and download information from untrustworthy sources. They should know how to differentiate between regular and phishing emails. A little media literacy training can also save you a lot of trouble.

Don't forget about the weakest link in your security chain: the human factor. Adequate instructions and training of employees who now access critical systems in the company from their home environment, potentially from private devices, should be implemented in your organization.

Knowledge about malware, viruses and phishing that is communicated swiftly and efficiently should help prevent negligent handling of the current threats that can threaten a company's existence.

TIP: ESET CYBERSECURITY AWARENESS TRAINING WILL PREVENT YOUR EMPLOYEES FROM ENDANGERING THE BUSINESS.



PART 3

6. TRAIN YOUR EMPLOYEES AND EMPATHIZE WITH THEM

We recommend you to share the following security tips with your employees.

HOW TO SPOT SUSPICIOUS INFORMATION SOURCES

- Publication date is missing
- The author of the article is missing
- The connection is not secure (lock icon missing in the URL field)
- The content is very emotional; many exclamation marks appear
- An immediate action is required; e.g., to buy something or share some data The content is full of grammar mistakes
- The content is graphic
- Phrases like "Why the media does not talk about this" appear

HOW NOT TO FALL FOR PHISHING SCAMS

- Evaluate the request. Is it a common one, or a suspicious one?
- If the sender uses the name of a company employee, contact this employee via a different reliable channel, or start typing a new email and insert the sender's address–have you ever been in touch?
- Don't accept files and do not click on anything in emails from complete strangers
- Before clicking on a website link, try to Google the website or even the name of the sender if the name does not sound familiar
- Look for grammar mistakes
- Do not send any sensitive information via email If possible, report suspicious emails

LEARN MORE ABOUT HOW ESET PRODUCTS BLOCK PHISHING.

CONCLUSION:

THERE WILL BE NO GOOD BUSINESS WITHOUT GOOD IT

The future of the workplace is digital. Here's why companies should focus on digitalization and great IT infrastructure, starting now.

CYBERTHREATS WILL RISE

The number of devices online is constantly rising and the tactics of cybercriminals constantly improving along with the use of sophisticated artificial intelligence to improve malware distribution and delivery. Gone are the times when phishing emails were very easy to spot.

The Hiscox Cybersecurity Readiness Report from 2019, which surveyed around 5,400 professionals from the US, UK, Germany, Belgium, France, Spain and the Netherlands, stated that around 61% of companies experienced a cyberattack in 2019, compared with 48% in 2018. "Globally, the median cost for the loss associated with a cyber incident has risen from $229,000 to $369,000," says the report. And the numbers are set to rise over the next years.

FLEXIBLE WORKPLACES WILL ATTRACT TALENT

More and more people require flexibility at work, which can be achieved by integrating online solutions and tools that will allow employees to work remotely.

A digitized workplace not only allows you to stay safe and productive in times of crisis–it also helps attract more talent, appealing mainly to millennials (born between 1980 and the late '90s), and Generation Z (born between the late '90s and 2010s), which is just entering the labor market. A Pew Research Center study from 2018 showed that in 2016, millennials became the largest generation in the US labor force, and it is therefore crucial to fulfil their needs, which among others include flexible working hours.

Another piece of research conducted by PwC stated that not only millennials but all generations of workers want more flexibility and a job that would occasionally allow them to work from home. "The similarities in attitudes across generations are striking," says the study. And so, when flexible and digitized solutions are implemented, employees of all ages can be more satisfied, motivated and productive.

CONCLUSION:
THERE WILL BE NO GOOD BUSINESS WITHOUT GOOD IT

REMAIN CRISIS PROOF

The COVID-19 crisis demonstrated that companies that were able to digitize their processes and assets withstood the crisis much better than the offline ones. Many experts agree that there are more crises and disruptions to come–thus, a remote workforce and both digitized and well-protected workplaces will not only be a competitive advantage, but also a necessity.

Hence, companies should realize that IT is their best business partner, and that in the future, they will not be able to operate without skilled IT professionals nor advanced cybersecurity solutions. The COVID-19 crisis may be a breaking point, one thanks to which society finally starts to perceive digitalization more positively. It's high time.

IF YOU WANT TO KNOW MORE ABOUT OUR EXPERIENCE, OR NEED HELP SECURING YOUR REMOTE WORKFORCE, LET'S HAVE A TALK. VISIT OUR DEDICATED PAGE TO CONTACT US DIRECTLY, AND WE WILL GET BACK TO YOU AS SOON AS POSSIBLE.