KVK
OCTOBER 2024

TAKE THE CYBER-SECURITY QUIZ!

SECURE IT!

GUIDE TO CYBER-SECURITY

JOIN OUR NETWORK ON LINKEDIN

- Protect yourself against BEC fraud
- Look, my online shop is OK!
- Entrepreneur Joost Fromberg was hacked: “We had no policy”
- Password do’s & don’ts

Connect with us!

Do you have questions about the online security of your business? Do you want to know how other business owners deal with cybercrime? Or do you have a technical cyber-security question? For answers and inspiration, you can also join us on LinkedIn. In the private group Cybernetwerk Ondernemend Nederland there are all kinds of cybersecurity experts who will be happy to advise you. Join the network by searching for the group Cybernetwerk Ondernemend Nederland on LinkedIn.

Discover more

Secure your business with the help of the articles and videos

Cybersecurity | KVK.

Colophon

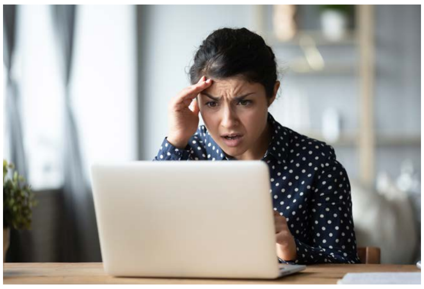
SECURE IT! is a publication from the Netherlands Chamber of Commerce KVK in cooperation with the Digital Trust Center.
Utrecht, October 2024

Contact
Questions or comments about the content of this magazine?
Email kvk.cyber@kvk.nl.

KVK

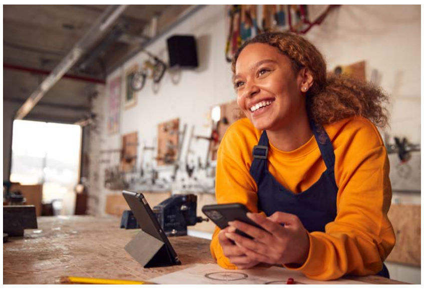
digital trust
center.

Contents



Virus panic!

We often shrug off a virus on our laptop. But 35 years ago, there was the first major panic about a computer virus affecting Dutch businesses. What kind of virus was it? And how did it end? **p. 10**



Protect your business with these 7 measures

Every business is different. Still, there are many security points that almost every business owner needs to think about. How cyber-resilient is your business? The Digital Trust Center lists 7 measures that you can get started on right away. **p. 18**

"We had no policy" – What Joost Fromberg learned from a hack

Joost Fromberg, owner of online marketing agency ODIV, was not concerned about the digital security of his business. Until his business was hacked and he had to deal with the consequences for months. What was the impact and what did he learn from it? **p. 30**

Password Do's & Don'ts

We need to use rock-solid passwords. But how long should they be? What can you use and what exactly can you not use? And how often should you change a password? Use these do's & don'ts to make it difficult for cyber criminals to crack your passwords. **p. 34**

And more

Introduction by KVK 4

Losing half your turnover to scammers this is BEC FRAUD 6

Hoppenbrouwers Techniek sees cyber-attack as a challenge 12

Cyber questions from entrepreneurs 16

Make your online shop more secure for customers 20

Cybersecurity quiz: test your knowledge 23

Join the DTC Community 24

Almost hacked! What happened when I took a phishing test 26

Introduction

Stay alert

Cybersecurity is no longer a new word. In fact, over the past 5 years or so, it has become one of the main security issues business owners have to deal with. Phishing, identity fraud, scamming, you name it. KVK itself has been named in many phishing attempts in the past few years. These target entrepreneurs to pay for non-existent 'urgent registration updates', for example.

If you receive a text message, email, or WhatsApp message asking you to renew a registration, pay a fine, or click a link, we sincerely hope that you know better than to just do it. But a scam can be incredibly convincing, as writer Liesbeth Sparks found out on page 26.

The damage done by a hacker or other cybercriminal cannot be overstated. A phishing mail may cost you money. But if you click a link that leads to ransomware invading your systems, you may lose all your client and sales information. Your reputation may also be irreparably damaged.

So, as fraudsters get cleverer and hacks become more sophisticated, what can you do to avoid falling into a cyber trap? The answer is not one piece of advice, of course. Yes, you need to install updates and use secure passwords. And make your employees aware of the dangers as well as their own behaviour. But there is so much more you can do.

Take a cyber scan to find out where the vulnerabilities in your business are, and act on the outcome. And, perhaps the most important piece of advice: stay alert! Once you have installed that state-of-the-art antivirus software, do not sit back and stop thinking about security. Keep working on it – just like you keep improving your product or services.

Do you have questions about any of the articles you read in this magazine? Do not hesitate to call the KVK Advice Team on 088 585 2222 or email kvk.cyber@kvk.nl.

Enjoy the magazine!

KVK

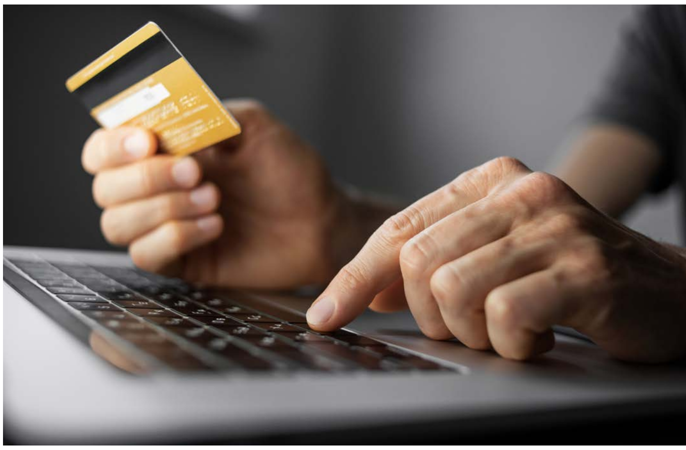
Stéphane Nappo
Vice President and Global Chief Information Security Officer Groupe SEB

"The five most efficient cyber defenders are: Anticipation, Education, Detection, Reaction, and Resilience. Do remember: Cybersecurity is much more than an IT topic."

LOSING HALF YOUR TURNOVER TO SCAMMERS THIS IS BEC FRAUD

BEC fraud is not a term you hear every day. However, according to the Public Prosecution Service in the Netherlands, BEC fraud is a growing concern. This email scam can cost you a lot of money – even if you run a small business. Learn more about BEC fraud and how to avoid it.

Early in 2021, a company from the Dutch town of Leimuiden made arrangements with a European supplier. After emailing back and forth, the company placed an order and received 2 invoices totalling €80,000. Until that point, it seemed like a normal business deal. In May 2021, the supplier contacted them to ask: “Where is the payment?” It turned out the company from Leimuiden had not transferred the money to the real supplier but to criminals. This was a real example of BEC fraud (article in Dutch).



1. What is BEC fraud?

BEC stands for Business Email Compromise. Criminals use your business email traffic to scam you. There are different types of BEC fraud, but 2 things are almost always part of it: the criminals use email, and they pretend to be someone else.

CEO fraud

A well-known form of BEC fraud is also called CEO fraud. In this, an employee receives an email from ‘the boss’, asking the employee to transfer a sum of money. In the end, ‘the boss’ turns out to be a criminal who receives the money. A well-known example is the Pathé case in 2018 (article in Dutch). The cinema chain unknowingly transferred a total of €19 million to criminals. And at the beginning of 2022, a Rotterdam steel company lost more than €11 million due to CEO fraud.

> “The moment you think ‘this is strange’, pick up the phone and call the sender.”

Invoice fraud

Another type of BEC fraud is invoice fraud. You get an invoice that you are expecting, but the account number on the invoice has been changed. The money you transfer does not go to your supplier but to the criminal. Sometimes the criminals even write in the email that the company has a new bank account number. They then ask you to update the account number in your accounting system.

Spoofing

How do criminals convince you that the mail comes from your supplier? “It may be that the email address has been spoofed, or even taken over”, explains Koen Hermans. He works as a prosecutor for the Public Prosecution Service and sees examples of BEC fraud every week. “Then you cannot tell from the email address that the email actually comes from someone else. But we also see a lot of ‘typosquatting’. That means the scammer changes a letter or number in the mail address. Nobody usually pays attention to that.” For example, if the real address is info@kvk.nl, the criminal might use info@kvk.nu. Or even @kvk.nI, where the last letter of the mail address is a capital ‘i’.

2. BEC fraud and small businesses

According to Hermans, BEC fraud is also a danger to smaller companies and foundations. "One report I saw was from a company that had an annual turnover of around €200,000. Because of the fraud, that turnover was halved. So yes, BEC fraud can happen to companies that do not have millions in turnover." In April 2021, the treasurer of a sports club (article in Dutch) received a payment request from the chairperson by email. It asked him to transfer €3,500. When the treasurer called the chairperson, it turned out they had not sent that email. "The moment you think 'this is strange', pick up the phone and call the sender", advises Hermans.

Financial losses

The actual losses caused by BEC fraud in the Netherlands are difficult to estimate, says Bert Feskens, a security expert at Security Delta HSD. "Few companies report cybercrime (article in Dutch) because they fear reputation damage or are embarrassed. So we are dealing with underreporting."

3. How to prevent BEC fraud

These tips will help you to prevent BEC fraud:

1. Put up technical barriers. For example, set up your accounting system in such a way that it is difficult to change an account number. Also, make sure the security of your email system is in order. Then it is more difficult for criminals to abuse your email address.
2. Use the '4 eyes principle'. Always have several employees look at invoices above a certain amount of money. Do you see something unusual? Then contact the supplier by phone to check the invoice. Never do this by email, as criminals may have hacked your mail server and intercept your email.
3. Create an open company culture. If employees are not afraid to ask you questions and can give feedback, they are more likely to report a suspicious situation. So an open attitude toward your employees can also prevent BEC fraud.
4. Pay extra attention during holidays. Criminals often strike when staffing levels are lower, during weekends or holidays.

4. Scammed! What now?

What should you do if you have been scammed through BEC fraud? Follow these steps:

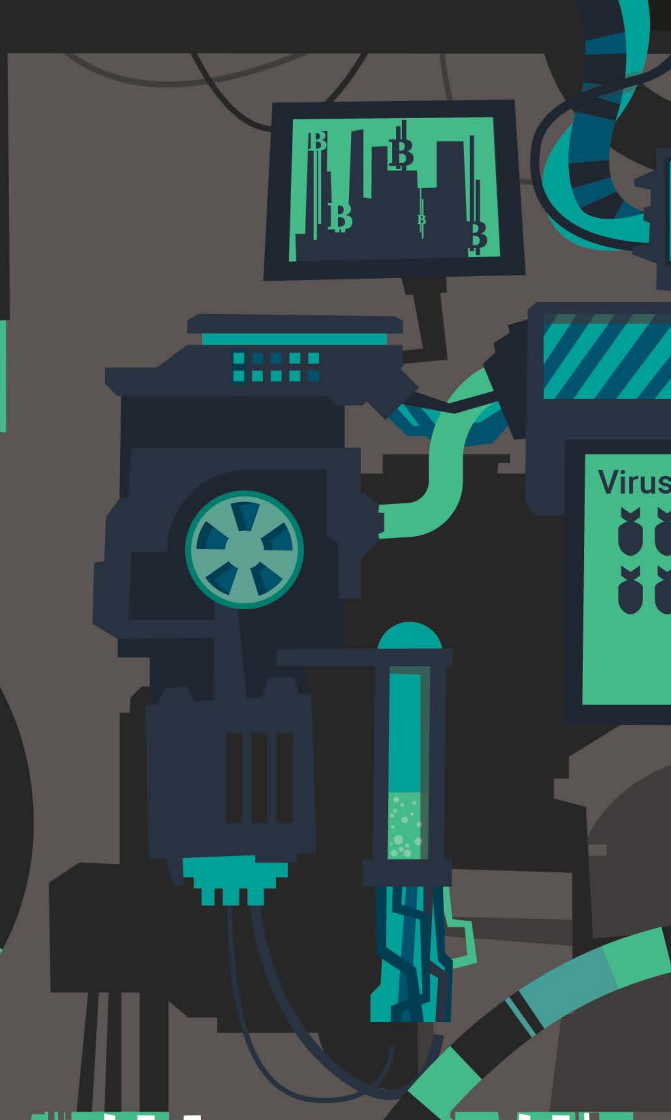
1. Call your bank immediately. Criminals usually move the money quickly to another account. But if you are on time, the bank may be able to transfer the money back to your account.
2. Contact your IT administrator, if you have one. Your email server may have been hacked. It is good to have an expert look into it with you.
3. Report it to the police. The police and the Public Prosecution Service can only take action when they are informed. If you do not report it, they cannot do anything against the criminals.
4. Report the fraud to the Fraud Help Desk. They warn other entrepreneurs about the latest scams.

Hack Help Desk

Have you been hacked or do you think you have been hacked? On Hackhelpdesk.nl (website in Dutch), you can find a step-by-step plan and practical solutions to prevent further damage. Also read the article 'Hacked, what to do?' on Business.gov.nl.

VIRUS PANIC!

We quickly shrug off a virus on our laptops these days. But around 35 years ago came the first major panic among Dutch businesses about a computer virus. A new virus would massively start erasing data, with dramatic consequences. “People will jump out the windows”, computer experts even warned. What was that virus? And how did it end?



1988 January

Virus discovered in Israel

Computer experts in Israel discover a new ‘electronic computer virus’. No one knows what it is, so the newspapers explain: “The term ‘virus’ is a technical term for a series of commands that start on their own. It can irreparably destroy all data on a computer.”

1989 January

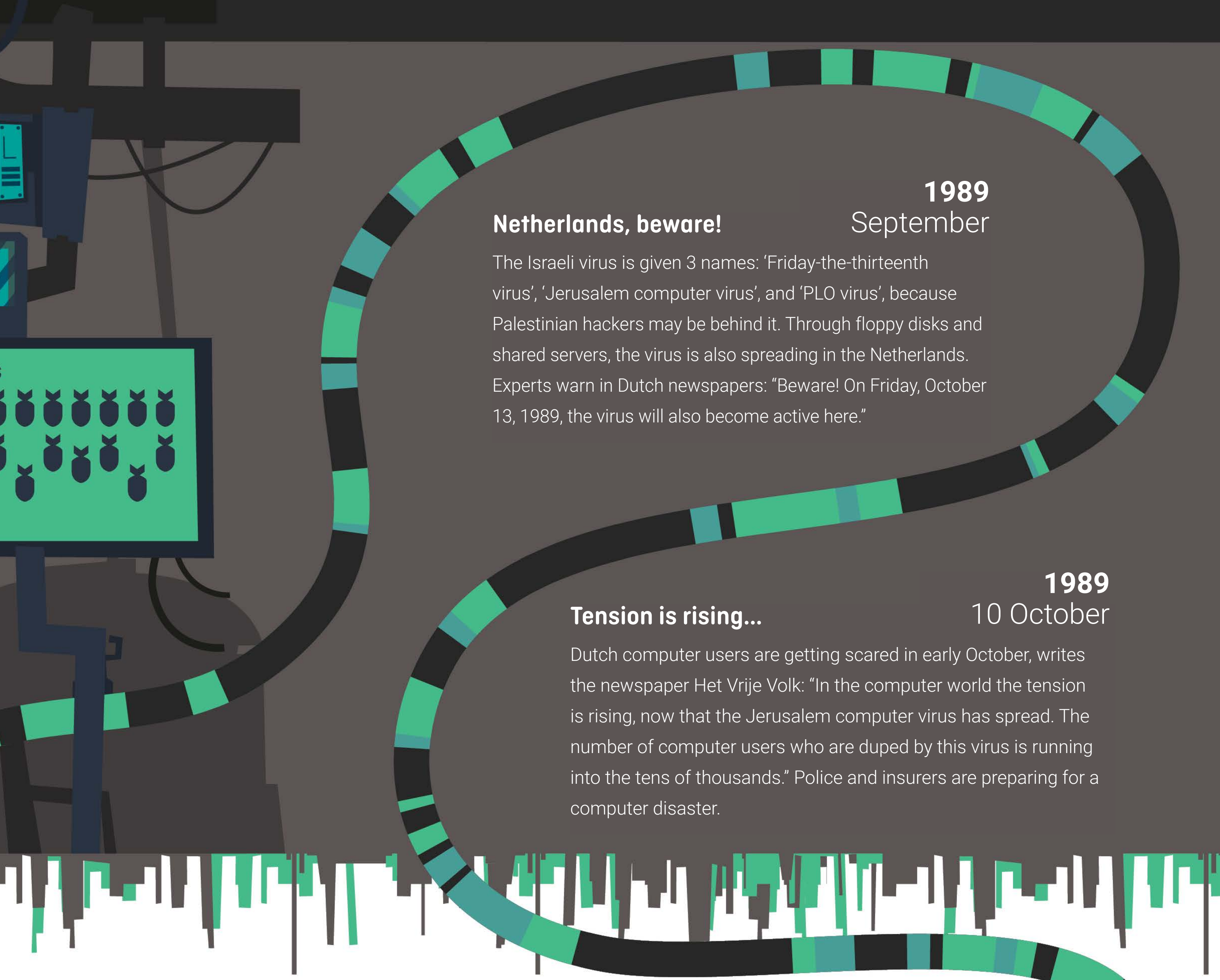
Chaos in England

The virus discovered in Israel turns up in early 1989 in England. “Computer virus wakes up on Friday the 13th”, writes the Nieuwsblad van het Noorden. At a number of British businesses, the virus destroys programs and data. This is causing “chaotic scenes”, according to the newspaper.

DID YOU KNOW?

1 One of the first computer viruses was called Ping Pong. If your computer was infected, on your screen you would see a little ball bouncing in all directions. It was discovered in 1988.

2 Around 1988, there were about 45 known computer viruses. In 2021, some 23.7 million new malware samples were discovered, about 65,000 a day.



Netherlands, beware!

1989
September

The Israeli virus is given 3 names: 'Friday-the-thirteenth virus', 'Jerusalem computer virus', and 'PLO virus', because Palestinian hackers may be behind it. Through floppy disks and shared servers, the virus is also spreading in the Netherlands. Experts warn in Dutch newspapers: "Beware! On Friday, October 13, 1989, the virus will also become active here."

Tension is rising...

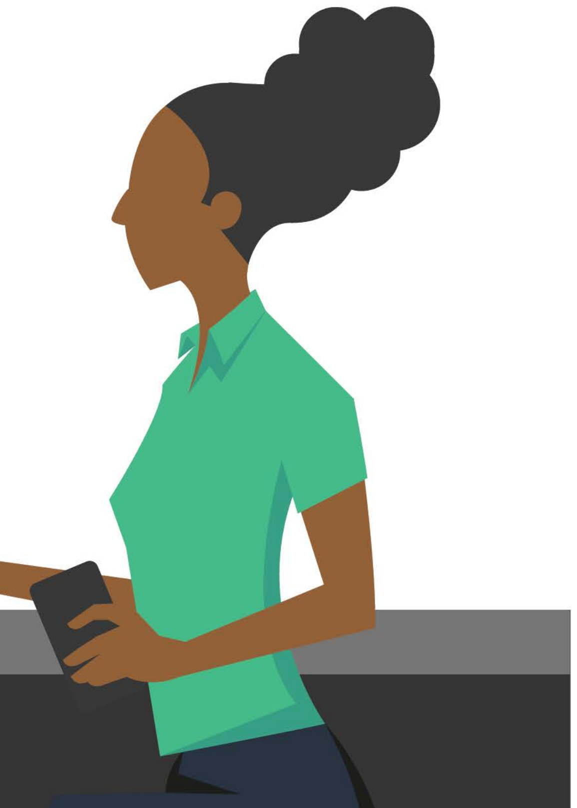
1989
10 October

Dutch computer users are getting scared in early October, writes the newspaper Het Vrije Volk: "In the computer world the tension is rising, now that the Jerusalem computer virus has spread. The number of computer users who are duped by this virus is running into the tens of thousands." Police and insurers are preparing for a computer disaster.

How does it end?

1989
14 October

In the end, it was not the big drama it was made out to be. According to the Telegraph, between 5 and 10 Dutch businesses were affected. In retrospect, according to the newspaper, all the panic seems to be "a storm in a teacup". That has an advantage, writes Het Vrije Volk: "Tens of thousands of unsuspecting computer users will be much more careful with their equipment from now on."



Did we learn anything?

Are you well protected against viruses and other forms of cybercrime? Find out on Cybersecurity | KVK how to work digitally safely and how to stay up to date on current cyber threats.

HOPPENBROUWERS TECHNIEK SEES CYBER-ATTACK AS A CHALLENGE

On Friday evening, the entire business was down. On Monday morning, everyone returned to work, more or less normally. Hoppenbrouwers Techniek fell victim to a cyber-attack in 2021 and worked really hard over a weekend to minimise the impact. Owner Henny de Haas feels remarkably positive about the experience: "I felt empowered by it."

The cyber-attack was discovered when an employee called the helpdesk on 2 July at around 18.30. He could no longer access his laptop. It soon became clear that the helpdesk itself was also having problems. "Then the conclusion was: we were probably hacked", says Henny de Haas. Hoppenbrouwers Techniek had fallen victim to a global cyber-attack. "The malware got in via an update to our Kaseya software, which allows us to manage endpoints and systems remotely. Everyone using this software who had installed the update was affected."

Finding a window

All this while De Haas thought he had armed himself well against cyber-attacks. "We had been insured against damage by hackers for about 4 years. Our security was certified, we use 2-factor authentication when logging in, and our computers are closely monitored. When joining the company, employees have to take an exam on all the rules around Wi-Fi, passwords, and so on. So, awareness among employees is quite high. Bu those hackers only need to find a window somewhere and they are in."

Everything could be infected

After the notification on Friday evening, the IT department contacted a specialised security company. "They started taking stock and making a plan of action for the coming weekend", he said. Once De Haas himself was alerted, he quickly understood that it was not just about the servers. "From the laptops to the security of the buildings, everything could be infected. In addition to the IT department, a lot of other employees have IT knowledge, so we created teams that all took care of part of the systems. Anyone who thought they could contribute something was invited to think along."

Webinars for staff

On Saturday, in every Hoppenbrouwers branch, a team of employees was busy checking computers, reviewing construction and installation projects, and calling mechanics. "By Saturday afternoon, we had solved 80% of the problems. Saturday evening, we were able to restore a backup and the server was slowly but surely cleaned up. By Sunday evening I was able to log in again. And on Monday we were able to get back to work." In between, staff and the outside world were kept informed. "With the help of the communications department, I presented 2 webinars, explaining to our staff all the steps we were taking. On a dedicated website, staff could read constant updates. And I also spoke to 5 radio stations and some TV stations."

> “In retrospect, I think we should have had a protocol and tested it. You practice fire drills too, don’t you?”

Demand for ransom

After the weekend, work resumed. “We called some more customers because some invoices had disappeared from our system. But apart from that, the damage was not very bad. The IT department and security specialists did spend over a week checking and cleaning up the last things.” And then, of course, there was the ransom demand. “This was a global attack on more than a thousand businesses and the hackers demanded 70 million in ransom. Should we have gone around with a collection bag? We did not respond and did not pay. We were busy enough plugging the holes.”

Practising emergency plans

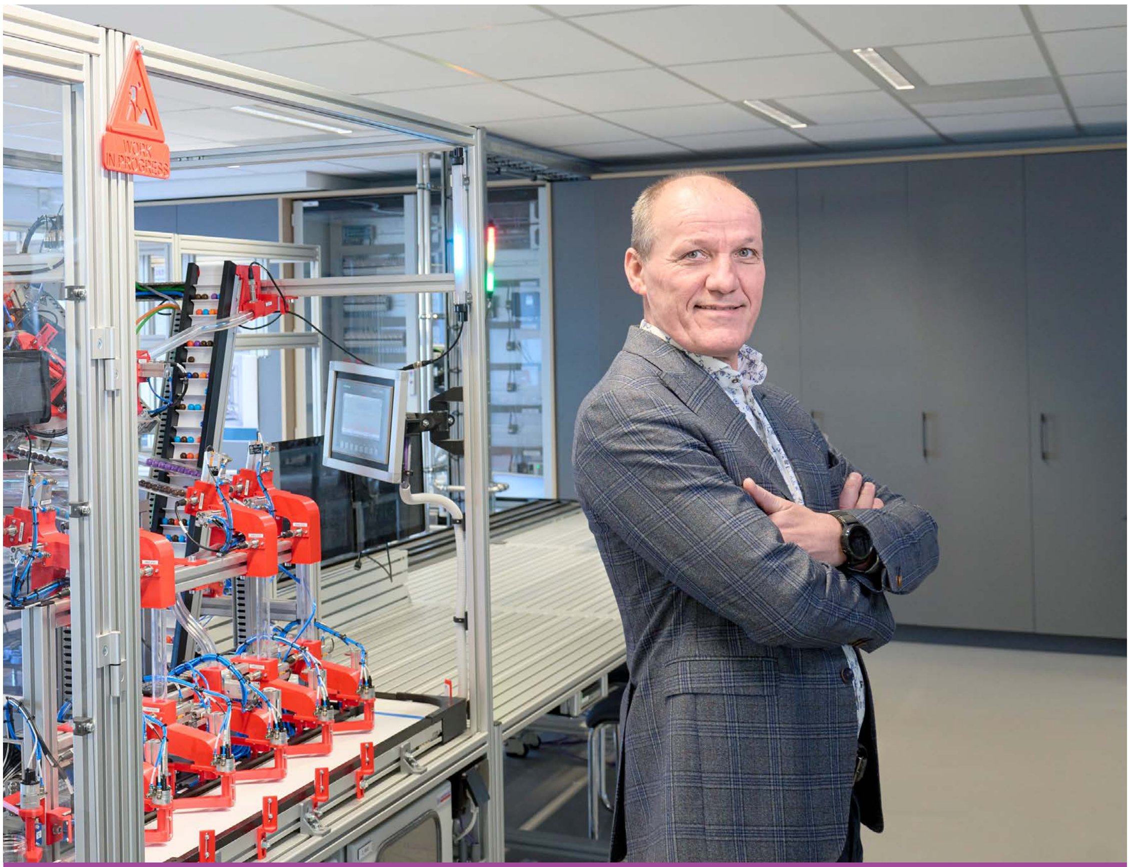
Looking back, De Haas is surprised at how his business acted so quickly. “We had no plan before about what we would do in such a case. But neither could I have imagined beforehand that we would develop an effective approach so quickly during that weekend. In retrospect, I think we should have had an emergency plan and tested it. Nobody does that, but that is crazy. You practice fire drills too, don’t you?”

Cohesion within the business

When asked what De Haas learned from this, a surprising answer comes: “It may sound crazy, but I would not have wanted to miss it. You do not wish this on anyone, but I learned a lot from it. In our business, we work in self-managing teams and responsibility is low down in the organisation, so employees are used to thinking along with the business. By bringing all those people together in a crisis, you organise so much brainpower, then the solution comes naturally. I found the unity that emerged in the business very moving.” In addition, awareness has become even sharper than before. “Because the chances of us getting hacked again are as high as anyone else. Of course, we monitor the systems even more closely, we have software that signals strange activity on the network, and we have our own cyber specialists. But when hackers really start looking, they will always find a weak point. Only, like with burglars, the company with the best lock might get passed by.”

Cyber-attack as a challenge

In any case, the setback has not made De Haas throw in the towel. The business has an ambitious vision for 2030 that is being implemented as planned, says De Haas. “We expect to triple our turnover and double the number of branches so that we have real national coverage. By then, we will have 5,000 employees, be 100% carbon-neutral and circular, and aim for an excellent customer experience. I see this cyber-attack as a challenge and I feel empowered by it.”



Henny de Haas

Director and owner of Hoppenbrouwers Techniek

Ever since he decided as a farmer's son that he wanted more than milking cows, he gradually made his dreams come true: from electrician, he eventually became manager director (2002) and owner (2013) at Hoppenbrouwers.

"I found the cohesion that developed in the business very moving."

- Hoppenbrouwers Techniek
- Total damage from cyber-attack: €500,000 (partly covered by insurance)
- 1,600 employees

Tip: "Do not leave everything to IT specialists, but learn about computers and security yourself. The whole world depends on IT and you should be aware of how vulnerable you are. Because so many of our employees have some computer knowledge, we were able to divide the tasks and tackle everything at once. This allowed us to get back to work quickly."

On Cybersecurity | KVK you will find the answers to the most surprising and unusual cyber questions from entrepreneurs. Do you have a cyber question? Ask us at kvk.cyber@kvk.nl.

CYBER QUESTIONS

Help, I've lost my laptop. What should I do?

Imagine: you return from a business trip. At the airport, you find out that your laptop is gone, with all your customers' data. A data leak, in other words. Maria Genova, expert in online privacy, tells you what to do.

Report the data breach to the Dutch Data Protection Authority
Customer data is privacy-sensitive information. According to the privacy act GDPR, you must report to the Dutch Data Protection Authority in such a case. If you don't, you can be fined up to a maximum of €820,000.

For customers, a data breach can have unpleasant consequences. So always inform your customers about the data leak and warn them about the risks. Criminals may send them phishing emails or make fake phone calls. Then, with the correct data they can empty your bank accounts. The best thing is to prevent a data leak of course. So secure your laptop with a strong password and encrypt your hard drive.

Ask your cyber question at kvk.cyber@kvk.nl.

> “Always inform your customers about the data breach and warn them of the risks”

Why should you not have your passport copied?

You are checking into a Spanish hotel or renting a sanding machine to spruce up your office floor. They ask: May I copy your ID? That is not without risk.

“That is because in the Netherlands we work with the citizen service number (BSN)”, says Frans van Berkel of the business PassProtect. “At birth you are given a unique citizen service number (BSN). That is the key to your identity.
If a malicious person gets his hands on that number, he can take out a subscription or take out a loan, or even rent premises for a cannabis plantation.” In other words, Identity fraud.

This is how to protect your data

- **Refuse to have a copy made**
  According to the privacy law GDPR, not just anyone can demand a copy of your passport. Only organisations that are legally obliged to do so, such as banks, insurers, or public authorities.
- **Make sensitive data unreadable**
  For example, with the government’s app KopieID. There are also various physical methods. For example, PassProtect has developed a removable film that you stick over your passport, driving licence or ID card. If someone then gets hold of a copy of your passport, your photo and citizen service number (BSN) are not completely visible. ANWB also offers such a product.

PROTECT YOUR BUSINESS: 7 TIPS

Every business is different. And there are several ways to work cyber-safely. But some security measures are the same for all businesses. How cyber resilient is your company? The Digital Trust Center (DTC), part of the Ministry of Economic Affairs, lists 7 measures you can take right away.

1 Make a back-up

Limit the damage of a cyber incident with a good backup. Make one or more copies of your business data. Keep at least one backup in another place. Think a safe or at your home. Do you have an IT service provider who takes care of this for you? Then ask for an overview of your copied company data at regular intervals. That way you know exactly what and how it is backed up.

2 Use multifactor authentication

Prevent someone else from accessing your account with multifactor authentication. Multifactor authentication is also called 2-factor authentication, two-step verification, or in short 2FA or MFA. It works like an extra lock on your account. You log in not only with your password, but also, for example, with your fingerprint, or a code you receive via SMS or an app. Enable this at least on your business email account and your most important business applications.

3 Turn on automatic updates

Software updates often include security updates in addition to user improvements. Hackers actively search for vulnerabilities in outdated software. So, do not wait to update your software and turn on automatic updates. In addition to your computers, think about your tablet, printer, and router.

4 Use antivirus software

Install antivirus software and make sure it stays up-to-date. Do this on all computers and servers in your business. Such a software programme detects and removes digital threats.

In addition, the software also indirectly protects the devices of, for example, your customers and suppliers. Many viruses use your email programme to spread out via your email traffic with others. So, antivirus software protects you as well as others.

5 Check your email security standards

Check the security of your email address via internet.nl. On this website, you can find out whether your domain name, the part after the @ sign, uses security standards. And which ones they are. Does your domain name not use security standards? Ask your IT service provider how to improve it. With good security standards, cybercriminals cannot misuse your identity to send spam such as phishing.

6 Recognise phishing

Phishing is a major danger to any business. With this form of digital scam, fraudsters trick you with fake emails, fake QR codes and fake SMS or WhatsApp messages. Make sure your employees recognise phishing. Practice, for example, with the online phishing quiz (in Dutch). Or start a phishing test in cooperation with an IT service provider.

TIP

Check the sender's email address. This is how:

- Take a close look at the domain name the email was sent from.
- Check that the domain name and the website address are the same.
- The difference may be well hidden. Can you spot the difference between mail@31008mailers.nl and mail@3I008mailers.nl?

7 Create an offline call list

Make sure contact details of important partners are printed out in case of a cyber incident. On the call list, put the details of, for example, an IT service provider, software supplier, and a cybersecurity company that will help you in case of problems. You can use DTC's example call list (pdf, in Dutch).

Make your business more cyber resilient

The DTC CyberVeilig Check (CyberSafe Check, in Dutch) is a tool that was developed especially for zzp'ers and SME businesses that have little experience with cybersecurity. In less than 5 minutes, you know where you stand and how you can make your business more digitally secure. Download your own to do list and get to work with practical instructions and tips.

LOOK, MY ONLINE SHOP IS OK!

Have you ever wondered how reliable your website or online shop appears to potential customers? If you do not seem trustworthy, few customers will want to do business with you. So, time to take a close look at your website. Do you appear reliable enough?

Customers are wary because scammers pretend to be honest entrepreneurs online. There are several ways to make your shop trustworthy for customers.

Quality marks

With a quality mark (keurmerk), you show your customers that you comply with the rules and regulations and offer a safe payment environment. There are various certified quality marks. Gerard Spierenburg, spokesperson for the Consumers' Association (consumentenbond), explains which quality marks inspire confidence in your customers. "We especially recommend consumers Thuiswinkel Waarborg or Webshop Keurmerk (in Dutch), because these quality marks have general terms and conditions, which have been agreed with us. Also, entrepreneurs who use these quality marks are affiliated to the independent Dispute Commission that helps with any conflicts between the webshop and consumer. Such a committee is quite a reassurance for many customers."

Even more effective

Now you might think: a quality mark, a seal of approval, that is the most important thing. But according to Michiel Henneke of Foundation Internet Domain Registration Netherlands (SIDN), consumers also pay attention to other things. Henneke conducted research into this. "We asked almost 4,000 consumers the question: what do you look for when you want to know whether a website is reliable? Hallmarks came third (51%), below reviews from other consumers (66%) and safe payment options (60%)."

A good online shop shows everything at a glance and does not leave the customer searching for quality marks, reviews, and payment options.

Reviews

Ratings from other consumers, or reviews, are the most influential factor, according to SIDN's research. Make sure reviews are highly visible on your site, so your customer can see reviews from other real customers right away. "It saves a customer searching for reviews themselves if you put them prominently on your site. That way, your customers stay in your site and do not move to, say, Google to read reviews there", Henneke explains.

iDEAL

That the payment option is important for customer's trust is striking, according to Henneke. "So, it is wise to look critically at your payment options. IDEAL has also become a kind of hallmark. Customers know that iDEAL properly checks which parties offer their service."

> "These days, you see many online shops sharing logos from review sites such as Trustpilot and Klantenvertellen. These are not really quality marks, but in the customer's perception they are similar. Or even better, because just having a logo from a trusted review site gives customers confidence."

Design and domain name

When it comes to appearing reliable to customers, you should not underestimate the design and domain name of your site, Henneke believes. "Cool if you have a quality mark, but if you can then hardly see it because it is the same colour as your website, it is of little use.

A good online shop shows everything at a glance and does not make the customer search for quality marks, reviews, and payment options."

A domain name ending in .nl inspires the most confidence among Dutch consumers. Do you also want to sell abroad, for example in Belgium? Then also buy .be as a domain name. That way you will gain the trust of your Belgian customers faster.

Trust

You don't want customers to drop out early because they don't trust things. That, according to Henneke ultimately comes down to. "The competition online is often cut-throat, you have to stand out. So, if you have a beautiful business, show your customers right away. Invest in the transparency of your business, you will reap the benefits."

Don't get hacked: 3 simple tips for a secure online shop

What can you do to make your online shop more secure? Marc van Vliet, security consultant at Perfect Day gives 3 tips to protect your online shop against digital threats. He worked in e-commerce for many years and knows the online dangers from practice.

1. Check what data you have from customers. "Many entrepreneurs do not realise how much customer data they actually have, or where they store it. You only know where to start with security once you know that. Also, do not ask for too much data from your customers. You do not need someone's date of birth to send them a mousepad." You do not have to secure customer data you do not have.
2. "Give your employees individual user accounts, with unique passwords." With a shared account and shared password, a malicious or careless employee is more likely to cause damage.
3. "Secure your contact form with a captcha (in Dutch). This is a test that proves a customer is not a robot." You can expect more spam and phishing emails if you do not secure your contact form properly. If you get fewer of those phishing emails, you are less likely to click on an infected link.

CYBERSECURITY QUIZ
TEST YOUR KNOWLEDGE

Do you know how to secure a weak password? Ever heard of hackers wearing coloured hats? And can you recognise a data breach? Test your knowledge and increase your cyber resilience. The letters accompanying the correct answers will eventually form a sentence.

1 Harmful software that a cybercriminal uses to lock your digital files and extort you is called?

○ C. Blackmailware
○ S. Ransomware
○ W. Spyware

2 Not all hackers are criminals. Ethical hackers detect security flaws at companies and report these to them. What is another word for an ethical hacker?

○ E. White hat hacker
○ Y. Green hat hacker
○ A. Black hat hacker

3 In this type of cyber-attack, criminals send so much traffic to computers, networks, and servers that they become overloaded. Websites and networks become very slow or even inaccessible. Very inconvenient if you have an online shop, for example.

○ T. Brute Force attack
○ C. DDoS attack
○ B. Spoofing

4 When you think of a hacker, you might think of someone behind a computer screen. But some attacks start with offline deception. For example, when a criminal enters your business premises by pretending to be someone else. Or you get a call from someone who is trying to get information from you, such as your password. What do you call this kind of deception?

○ O. Physical harassment
○ E. Offline virus
○ U. Social engineering

5 Public wifi networks such as on the train or at an airport are unsafe. As soon as you log in to such a wifi network, a hacker can access your device. In what way can you use public networks more securely?

○ R. By using a VPN. With it, you are more anonymous on the internet.
○ E. By using a firewall that blocks attacks.
○ T. By using blacklisting. This makes your device invisible to hackers.

6 Cyber specialists call this the weakest link in cybersecurity.

○ V. Weak passwords
○ E. People
○ P. Bad antivirus software

7 What is the best way to make a weak password like 'hello123' more secure?

○ L. Save the password in a password manager.
○ U. GUse it for only 1 account and share it with no one.
○ I. Turn on two-step verification.

8 Which of these cases is a data breach?

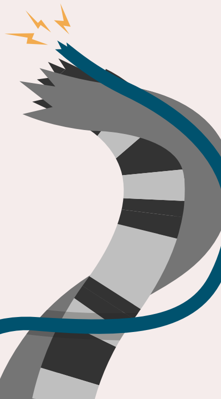
○ N. You have not backed up for a year.
○ M. You turn off your laptop before a software update is completed.
○ T. You send a confidential email to the wrong person.

Enter the letters of your answers here. .

□□□□□□□□ **!**

Answer

You will find the answer on p. 35.



JOIN THE DTC COMMUNITY

The Digital Trust Center has a trusted online community where knowledge, information, and experiences around cybersecurity are shared. The DTC Community is for entrepreneurs and IT specialists in the Netherlands.

Sign up and stay informed about serious security breaches. By joining this community, you increase the digital resilience of your organisation and contribute to a safer Dutch business climate.

Will we see you soon at the DTC Community? Go to digitaltrustcenter.nl/community (in Dutch).

What to do in the event of a cyber incident?

Go through these steps if you are dealing with a cyber incident

1. **Stay calm**

2. **Call your IT helpdesk**

3. **Discuss**
   a. whether or not your internet connection remains available
   b. whether your systems should be switched on or off

4. **Make an inventory of what still works**

5. **Record all actions and activities in a logbook immediately**

digitaltrustcenter.nl

digital trust
center.

ALMOST HACKED!

WHAT HAPPENED WHEN I TOOK A PHISHING TEST

Chances are you got one recently: a weird email from a stranger, or a text message about a delivery when you did not order anything. Phishing is a part of life. But do you recognise every suspicious message? I did a phishing test and found out that some phishing emails are truly convincing.

Liesbeth Sparks
Content creator at KVK

As a historian, I know very well what went wrong in the past. But we are also unsafe in the 21st century. In this series, I examine today's risks. How do we protect our businesses against cybercrime? I talk to experts about that.

Sometimes I wonder if anyone ever falls for one of those emails from a 'dr mike paul'. From Burkina Faso, he asks for your personal details. In exchange for 10 million dollars. Don't think so, pal. That email goes straight into the bin. But even if you recognise some phishing easily, it is still a big problem. "Around 90% of all data breaches worldwide start with a phishing message", says security expert Dim Gerssen. Time to test how cybercriminals operate. Do I fall for a really good phishing email?

March - Fake phishing

"That's agreed then", says Gerssen on the phone. Security company Surelock will send me and 2 of my colleagues phishing emails in the coming period. Or rather: fake phishing emails. The security company trains entrepreneurs and their employees with so-called phishing simulations. If I click on a 'suspicious' link in such a fake email, I do not end up with malicious software, but with the message: 'You have been phished!' Hopefully I will not fall for it ...

April - Everything is suspicious

After the conversation with Gerssen, I see hackers everywhere. I check every email with an unknown sender 3 times. A few mails I bin straight away. I am not the only one on my team who no longer trusts anything. "I am completely paranoid", laughs colleague Hajar.

But it does take a long time, this experiment. After a few weeks, I have not received any really suspicious emails, and I stop paying such close attention. "That is quite normal", says Gerssen. "At the beginning of a simulation, it is constantly on your mind. But over time, your attention slackens. German scientists saw a decline in alertness in test subjects 6 months after a simulation." And cybercriminals benefit from your momentarily not paying attention. According to the Dutch Banking Association (NVB), the damage caused by online scams in the Netherlands in 2021 was as much as 62.5 million euros.

September - The test

'Ping'. I am in the office, a cup of coffee next to me. Hey, an email from Hajar. Weird, I am not expecting any news about our project. And is that a link to a pdf? I move my mouse to it, but linger for a moment. This is not right. "Hajar", I say. How convenient that she is sitting opposite me. "Did you just send me an email?" She looks at me questioningly. "Huh? No."

Shock hits us. I consult with my teammates. 2 others have also received the mail from 'Hajar'. We file a report to IT. I mull over: who is behind this? Only after half an hour do I think: could this be the phishing test? I wipe sweat from my forehead while calling Gerssen. Meanwhile, our security department examines the email. On the screen they read: 'You have been phished!' That was a close call.

LinkedIn

When I get Gerssen on the line, I do have a few questions. For instance, how did he know that Hajar and I work together a lot? "Through LinkedIn", he explains. That is right, we often respond to each other's posts. Could I have prevented this? "No, not really", says Gerssen. "There is always something known about a business: through social media, news pages, or in this case employees posting to others." So, you definitely need to be careful what you share, but it is even more importan to recognise that something is wrong when you receive a phishing email.

Gut feeling

I work so much with my colleague Hajar that I know her emails better than anyone else. This message did not 'sound' like Hajar: that is why I did not click on the link. "That gut feeling is the basis", says Gerssen. "I could say: 'always check the sender's email address', but you probably do not pay direct attention to that. Do you sense something is wrong? That is the moment to check the mail thoroughly. So, when in doubt: do not click, but stop."

What you can do:

- Check the sender. If it is a strange or unknown sender, or a weird variant of an official email address, throw away the email. Or have it checked by your IT administrator.
- Check the link or attachment. If you hold the cursor over the link, you can see where it leads. Or google the company name in the link.
- Call or email the sender. Do not reply to the email you received, but find contact details via an official website or your own contact list.
- Compare the mail with the latest sample phishing emails (in Dutch) on Fraudehelpdesk.nl.

Effort

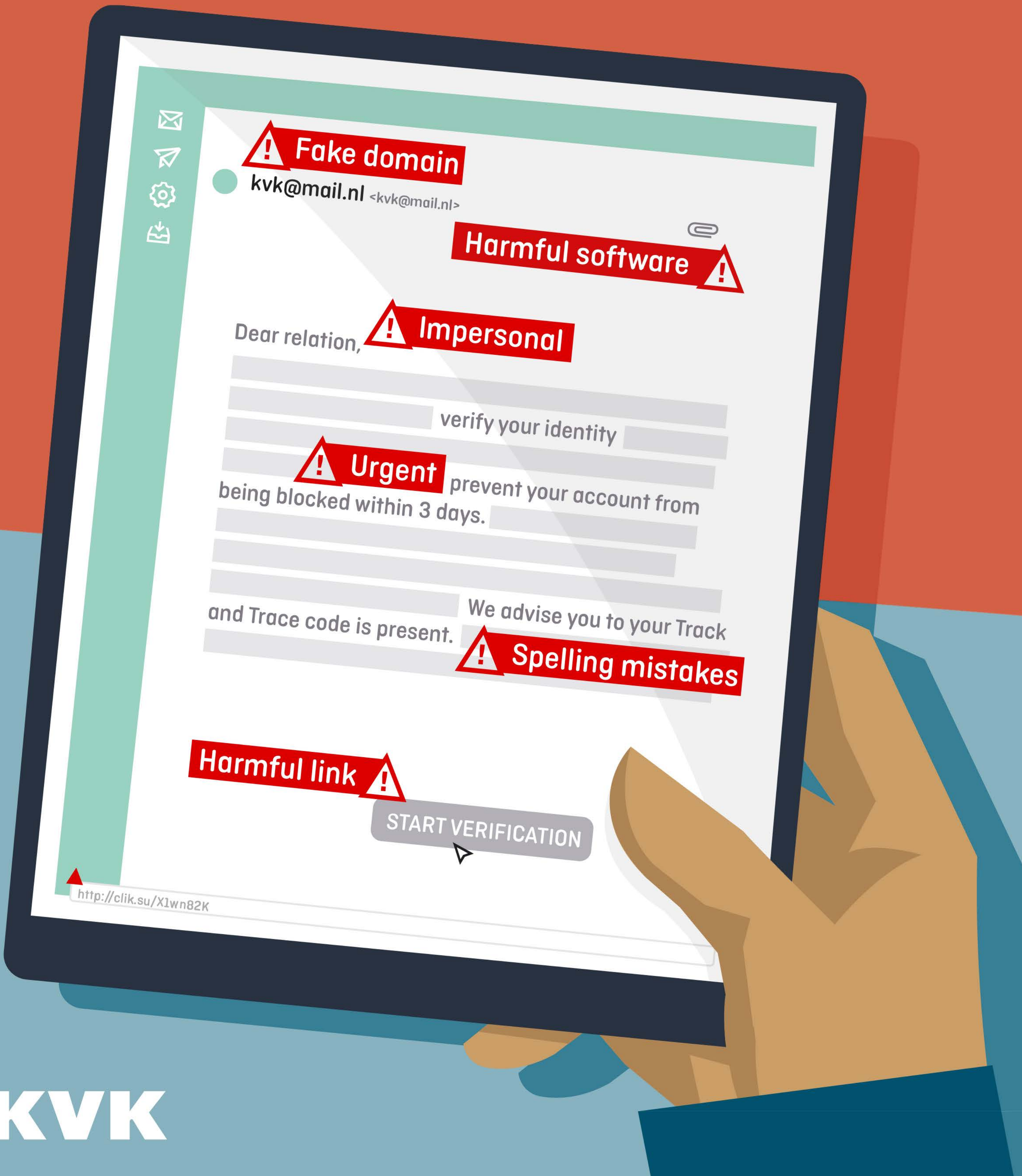
'Is a criminal really going to research that much information about me for one email?', I wonder. "In a small business with 10 employees, the risk is not so great. But in larger businesses it certainly happens", Gerssen replies.

Criminals attack small businesses by shooting with hail. They buy up email lists, for example on the darkweb. They send phishing emails to all the addresses on those lists. "So, if your business email address is on such a list, there is a good chance that you will get a phishing email", he says. And if the first one fails, they just try again. And again.

October - Paying attention

It had an impact on me, this test. I had thought: 'bring on the fake phishing email'. But I really almost fell for it. How useful such a simulation is in the long run, experts disagree. It seems that just receiving a fake email is not enough: business owners and employees need more knowledge and information to recognise phishing. Special training courses could help with this. In any case, I will be extra careful in the coming period.

HOW TO RECOGNISE A PHISHING MAIL



kvk@mail.nl <kvk@mail.nl>

Dear relation,

verify your identity

prevent your account from being blocked within 3 days.

We advise you to your Track and Trace code is present.

START VERIFICATION

http://clik.su/X1wn82K

KVK

‘WE HAD NO POLICY’

WHAT ENTREPRENEUR JOOST FROMBERG LEARNED FROM BEING HACKED

Joost Fromberg, owner of online marketing agency ODIV, was not concerned about the digital security of his business. He preferred to help clients build and optimise websites, social media, email marketing, and data analysis. Until his business was hacked last summer and he had to spend months dealing with the consequences. What exactly happened, what was the impact, and what did he learn from it?

You were hacked. How did that happen?

"It started off quite innocently. A colleague said: 'Hey, someone is doing something with my mail. I get a message that someone is in my private mail and I can't get into it myself anymore.' The password and two-factor authentication were no longer working. He couldn't access anything anymore. Our Facebook Business Manager account appeared to be blocked. We use this tool to display customer ads on Facebook and Instagram. Linked to this tool was the private email of our colleague. Around 130 ad accounts of our customers are listed in Facebook Business Manager with their credit card details. At that moment, we saw emails coming in and it went on and on. We could no longer access the data ourselves, but we saw that ads were being placed with a budget of 5,000 euros a day. Panic ensued. We had been hacked."

Headless chicken

"What should we do? The first day we were running around like a headless chicken. We had never experienced a hack, nor did we have a policy in case we did. A step-by-step guide of what to do in such a situation, we didn't have one. My colleagues and I locked ourselves in a room and tried to find out which accounts had been hacked. We called those customers and asked them to immediately block their credit card or remove the payment method. Facebook books payments several times a day, a few hundred euros each time. So if you act quickly, you can limit the damage."

An exhausting process

"It took a lot of time to call all customers. We also had to approach customers where we hadn't been active for a long time. Fortunately, the financial impact was limited. Then came the question: how do we ensure that we can go on with our Facebook ad accounts? The history and data of customers were stored there and we wanted to keep those. The contact with Facebook was a drama. Every time we got a new customer service representative, who didn't understand a thing. We were referred every time and there was really zero help. An exhausting process."

What was the impact of the hack?

“The impact for our business was huge. Resolving the hack took us about 6 months. The first time, we were mainly concerned with informing customers and keeping track of those calls. In retrospect, I should have done this differently. Because we didn’t start off by keeping a strict record of which customer we had already informed and which not, it took us a long time. Had we logged better, we could have crossed off files. It remained a bit of chaos. Then again, we also didn’t know how long it would take to handle the hack.”

Admitting mistakes

“Towards our customers we have always been transparent. If you have been working together for a while, admit your mistake, and want to work together on a solution, you can count on a lot of understanding. One customer said: it is a little annoying for me, but for you, with 130 customers, it is much worse. We did not lose any customers because of the hack. Then we involved the police, because there was **identity fraud**. But try explaining to a policeman how Facebook, ad accounts, and email work together in our case. The report did not get us anywhere. We were really lucky that our customers were not financially duped in the end. Facebook made sure the money was refunded. But cybersecurity is clearly an industry in its infancy. You are completely on your own.”

What did you learn from it?

“My business ODIV has been around for 6 years. Until the hack, we were not concerned with our digital security. After the hack was resolved, we started working hard on our security. We first took care of some practical things. For instance, we set up a password manager for all colleagues, with free accounts for family and friends, so that they too become aware of the importance of secure passwords.”

Sharing experiences

“Then came the question: what is our role towards customers? We don’t want customers to have the same experience we did. Cybersecurity at SME businesses is often not in order. And they do not have access to a lot of information. There is no step-by-step manual with prevention or escalation policies. Therefore, we have summarised and recorded our findings and experiences in a white paper. This white paper is a report that presents a problem and offers a solution, and it focuses on 2 questions: ‘How do you make sure you don’t get hacked?’ and ‘What do you do if you do get hacked?’. If we notice that customers are careless with passwords or transmitting data in an insecure way, we engage with them. We are now looking at starting breakfast sessions or lunch & learn sessions. The angle is: this happened to us, this is what you need to take into account and this is what you can do.

> “If you have been working with each other for a while, admit your mistake, and want to work together to find a solution, you can count on a lot of understanding.”

“We have turned the hack into something positive and are happy to share our experience and knowledge with other entrepreneurs”

We want to make as many businesses as possible aware of digital security and provide a step-by-step guide for emergency situations. We hope not to experience what happened to us again. We have turned it into something positive and are happy to share our experience and knowledge with other entrepreneurs. Digital security has become an important part of our business.”

Tips from Joost Fromberg

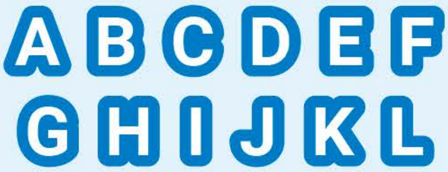
- Disconnect your private email addresses from your business accounts.
- Be prepared for a possible hack and make a step-by-step guide.
- Do not think it won’t happen to you: it is not about how big your business is, but how easy you are to hack.

Password

Tips for a strong password

& Do's Don'ts

Do's



Use long passwords or passphrases, preferably more than **12 characters**.

Use **lowercase, uppercase, numbers, and special characters.**

Choose nonsensical combinations that **only make sense to you.**

(E)ntrepeneurship
(I)s
(F)un

Use an **acronym**, take only the first letters of a sentence and join them together.

D30dorant

Replace one or more letters with **a number.**

Don’ts

duplicate
duplicate
duplicate

Repeating passwords for multiple accounts.

1234567890

Using **obvious words or sequences**.

Never changing your passwords.
Do this at least once a year.

Candlestick231!

Putting capital letters in a **predictable place**.

30_12_92@1!

Using **Personal information** such as Your date of birth, name, or address, or the name of a family member.

The answer to the quiz on p. 23 is SECURE IT

KVK