How to fight back against common scams

Ebook

pxp

Contents

Introduction 3

How to fight back against phishing attacks 4

How to fight back against CEO fraud 7

How to fight back against malware 10

How to fight back against ransomware 13

How to fight back against DDoS attacks 16

How to fight back against SQL injection attacks 18

How to fight back against credential stuffing 20

How to fight back against third-party supplier attacks 23

How to fight back against terminal swap-out fraud 26

How to fight back against Covid-19 scams 29

Conclusion 32

How to reduce data security risk 34

Introduction

Welcome to the first edition of How to fight back against common scams. Technology has helped us trade with others beyond those we can see. It has evolved trust beyond those we know. However, while it provides great opportunities, it also comes with risks. In fact, opportunities and risks are two sides of the same technol- ogy coin; they are integral to one another.

Technology enables us to innovate to increase revenues, cut costs and improve services. It also opens us up to criminal abuse and the business disruption, negative publicity and financial loss that may result. This booklet has been developed to help you take the necessary steps to protect your business and customers against criminals. It contains a number of revised articles from our popular 'How to fight back against...' series, originally published on the PXP blog.

Criminals are unscrupulous opportunists so we've added a section about how scammers have capitalised on the Covid-19 crisis. I hope you find this booklet a useful source of practical advice as well as food for thought as to how to approach security within your business.

Graeme Zwart Head of Security at PXP

How to fight back against phising attacks

Phishing exploits the human element and is one of the main attack vectors for various types of cyberattack. Businesses should place particular emphasis on countering it. What is it? Phishing is when criminals send e-mails purporting to come from reputable sources to trick recipients into revealing personal information or installing malware.

How does it work?

The attack vectors for this type of social engineering may vary. Approaches could come via a phishing e-mail, via SMS when it's known as smishing, or voice call known as vishing. Regardless of the attack vector, the aim is the same. Criminals want to steal personal and financial information to commit identity theft, make financial transfers or fraudulent claims, or to sell to others. Most phishing campaigns employ one of two basic methods. Either they want recipients to open attachments that contain malware. Or to click on links to websites that are often clones of legitimate ones. These are set up to harvest data or to deploy malware. The cover story may also vary. Criminals may impersonate banks, the police, tax office, government agencies and suppliers. They target large numbers of

recipients and rely on only a few falling victim. Spear phishing is a more targeted form of phishing, which we cover in the section on CEO fraud. What's the impact? Phishing attacks can culminate not only in loss of data but also loss of financial value. That's through business disruption, regulatory and card scheme fines, loss of company value, loss of customer trust and reputational damage. How can businesses protect them- selves? Your staff are one of the first lines of defence against phishing attacks. They are also one of the biggest vulnerabilities because they are of- ten the target and are fallible. Crim- inals are master manipulators so strengthening your human defences should be a key part of the fight against phishing attacks.

1.. Train your staff

Awareness that these scams exist and how they work is half the battle. Brief your staff on how to recognise phishing scams. And to delete the e-mail and report it, if they receive contact they're not expecting or don't know the sender. Advise them not to click on links, open attachments or call any telephone numbers listed in such e-mails.

2. Know the psychological triggers E-mail phishing scams are re- al-world con-tricks transferred online. Criminals prey on victims' fear, greed, curiosity, naivety or just the human desire to be help- ful and professional in a work- place setting. Or they try to cre- ate a false sense of urgency by claiming that your business has been a victim of fraud or that your account will be disabled. Be wary.

3. Test the effectiveness of training Simulated phishing attacks will help you determine the effectiveness of staff awareness training, and which employees might need further education. Build a positive security culture by making it easy to report suspected phishing attacks without fear of blame.

4. Implement appropriate technical measures Deploy e-mail filtering and web filtering to block malicious web- sites. Use monitoring systems to inspect and analyse web traffic. Install anti-virus systems. Ensure that remote and working from home procedures are sufficiently secure and robust.

5. Stay up-to-date
Keep all systems current with the latest security patches and updates. Criminals are cunning and consummate opportunists, so stay up-to-date on current phishing strategies. Keep security policies and procedures under constant review to ensure they address threats as they evolve.

How to fight back against CEO fraud

No-one likes to disobey or challenge instructions from their boss. This social engineering scam exploits that.

What is it? CEO fraud, also known as business e-mail compromise, 'bogus boss' fraud or spear phishing, is a targeted form of phishing. It's when criminals impersonate company executives to trick staff into making unauthorised funds transfers, revealing sensitive information or installing malware.

How does it work? Criminals 'spoof' e-mails so they look as if they come from the CEO, CFO, HR director or other senior executive. Or they hack the address to take it over. They instruct the recipient to transfer funds to complete a deal or pay an in- voice. Any funds transferred go directly to bank accounts controlled by crimi- nals. Or they ask for personal, tax or financial details of colleagues, which they can monetise. Criminals may apply pressure by saying the request is urgent. And try to pre- vent recipients from raising the alarm by saying it is confidential, commercial- ly sensitive or should not be discussed with colleagues. Variations on CEO fraud include the supplier swindle. This is when criminals send e-mails purporting to be from suppliers with a change of bank account details. They request payment to an alternative account.

However, this is not your supplier and the new bank account is controlled by criminals.

The supplier swindle can happen in reverse. Criminals contact your suppliers pretending to be an employee of your company. They inform them that your bank account details have changed and supply new ones (their own). The first you know of this may be when a supplier contacts you to chase an unpaid invoice. Impersonation of professional services firms is also a popular ruse. Criminals pretend to be a law or accountancy firm, claiming to be handling time-sensi- tive or confidential matters on behalf of your company.

They request a quick or secret transfer of funds. What's the impact? CEO fraud is a serious and growing problem worldwide. It cost companies more than $1.8 billion in losses in 2020, according to the FBI. It affects all types of companies: large and small, well-known and less well-known, in all industry sectors. Google and Facebook were stung for $100 million in CEO fraud, the BBC reported in 2017 What can businesses do to protect themselves?

Your staff are one of the first lines of defence against phishing attacks. They are also one of the biggest vulnerabilities because they are often the target and are fallible. Criminals are master manipulators so strengthening your hu- man defences should be a key part of the fight against phishing attacks.

1 Make preliminary checks Check sender e-mail addresses by hovering the mouse cursor over them. Also check that they are spelt correctly and come from a corpo- rate account rather than one that resembles a corporate account, or from a free e-mai l service, such as gmail.com or yahoo.com.

2 Verify suspicious or time-sensitive requests If a request is made for a wire transfer, bank details or personal infor- mation, verify this with the organisation or individual making the request using established contact details. Do not reply to the e-mail or use tele- phone numbers provided in the e-mail — they may be fake.

3 Implement secondary sign-off Implement some form of secondary sign-off internally for changes in payment information. Consider two-factor authentication for the corpo- rate e-mail system to raise the bar against criminals.

4 Know your customers and suppliers Know the habits of your customers and suppliers. This will give you a better chance of spotting out-of-the-ordinary requests or sudden chang- es to business practices. Be suspicious of requests which seem urgent, secret or arrive unexpectedly at the end of a business day or week, and pressure you to act quickly.

5 Moderate social media postings Be wary of what you post online to social media, company websites, especially job titles, organisation charts and out-of-the-office contact de- tails. It's very easy for a criminal to create a spear phishing e-mail from information gained through a simple internet search.

How to fight back against malware

Malware is another of the main ways for various cyberattacks to spread. The costs to your business go be- yond direct financial loss and include the indirect costs of loss of brand value, reputation and trust. What is it? Malware, short for malicious soft- ware, is a blanket term for viruses, worms, trojan and other harmful computer programmes. How does it work? Malware can infect a computer or network from a number of sources. These include contaminated e-mail attachments, infected websites whether visited directly or clicking on links in e-mails or social media posts, or from corrupt files stored on external devices, such as laptops, mobile devices or USB sticks at- tached to the network. Criminals use malware to read, copy or export data from computers or systems. They can then sell the data. Or use it to commit identity theft against individuals or extortion against businesses.

Criminals can also use malware to gain control of a device or network. This is useful for activities where large compute power is needed, for example launching distributed denial of service (DDoS) attacks or mining bitcoin or other cryptocurrencies. What's the impact? The impact of a malware-induced data security breach could be se- vere. This includes breach investiga- tion costs, fines and negative public- ity. As with DDoS and ransomware attacks, there is also the impact of business disruption, recovery time, lost productivity and sales, if your website is offline or your business is otherwise unable to trade. What can businesses do to protect themselves? If your business is maintaining a robust level of security, you have a good chance of fighting back against malware. Here are our top ten tips.

1 Raise awareness Educate your staff on the malware threat and what they can do to keep themselves and the organisation safe. Forewarned is forearmed.
2 Keep anti-virus/malware current
3. Screen e-mails and attachments. Make sure your software is set to 'automatic update' to get the most recent protection.
4 Protect installations and configurations
5 Password-protect the configuration of software. One of the first things that hackers do when breaking into systems is to escalate their privileges to administrator level. No-one should be able to disable or alter configurations without authorisation.
6 Restrict web browsing.Reduce the chance of staff visiting unsafe sites which could contain malware.
7 Prevent staff using unauthorised USB sticks. These can more easily transmit viruses to computer equipment.
8 Segment your network. Prohibit direct public access between the internet and your point-of-sale
and payment system. Only permit what is necessary for sales and card processing.
11 Check firewall coverage
12 If you change anything on your network, ensure that all devices, including mobile and employee-owned devices, are still protected by the firewall.
13 Patch software regularly
14 Review your patching regime regularly, too.
15 Scan for vulnerabilities across your network.
16 Have a supporting process in place to action any vulnerabilities reported.
17 Encrypt sensitive data.
18 Do not store sensitive card data unless strictly necessary. Encrypt data in transit and at rest so there is less data to worry about.

How to fight back against ransomware

Ransomware attacks against businesses are on the rise. Protect against the business disruption they cause. What is it? Ransomware locks computers or encrypts files, preventing users from ac- cessing their devices or data, and demands money from victims to regain access. How does it work? Ransomware is typically installed when a user clicks on a malicious link, opens a file in an e-mail that installs malware, or via a so-called 'drive-by' download when the user visits an infected website. Alternative attack vectors for ransomware include exploiting vulnerabilities in software or external-facing infrastructure, brute force attacks, or compromis- ing managed service providers. What's the impact? Businesses are now firmly in the cross-hairs of criminal ransomware gangs. That's because they have deeper pockets and more incentive to pay ransoms than individual consumers.

The fully-loaded costs to a business of a ransomware attack are far bigger than the cost of the ransom. They include the direct costs of business disrup- tion, recovery time, incident response, fines and breach notification. There are the indirect costs of loss of brand value, reputation and trust. And finally, the opportunity costs of lost productivity and commercial contracts. Ransomware attacks have recently evolved to encompass 'double extortion'. This is where criminals not only block access to systems and data but also threaten to release sensitive information, unless a ransom is paid. The Fi- nancial Times reported a 200 percent increase in victims of double extortion attacks between June and October 2020. So, ransomware is not a problem happening elsewhere to other businesses. It's very much happening to you and your peers.

Travelex suffers £25 million profit hit after attack Travelex, the currency exchange busi- ness, fell victim to a ransomware attack in December 2019. Criminals demanded £4 million to restore systems and prevent data, including sensitive card data, from being leaked online. Operations were reduced to pen and paper. The resulting disruption, combined with the effect of Coronavirus, knocked £25 million off Trav- elex's profits and put its parent company under significant financial pressure.

How can businesses protect themselves? If your business is maintaining a robust level of security, then you have a good chance of fighting back against ransomware threats.
1. Screen e-mails and attachments, quarantining any dangerous ones
2. Restrict web browsing to reduce the chance of staff visiting unsafe sites, which could contain malware.
3. Prevent staff from using unsanctioned USB sticks in company equipment
4. Segment your network to help contain and minimise the spread of ransomware-containing malware in the event of an infection

5. Back up data and check the integrity of those back-ups regularly
6. Patch software regularly and review your patching regime regularly The tips mentioned here are by no means exhaustive. Many of the policies and practices required for PCI DSS, the global data security standard adopted by the card schemes, are directly relevant to combatting ransomware. Revisit them to ensure that are still fit-for-purpose. Roll them out to the rest of the business, if they're not already. Good processes and technology will take you about two-thirds of the way towards securing your business. The multiplier or accelerator effect comes when you add people. So, train your staff. Ensure that they are familiar with current phishing attacks, including person- ally addressed spear phishing and business e-mail compromises, also known as CEO fraud. It's also worth conducting test phishing attacks to reinforce learnings and hone training methods.

How to fight back against DDoS attacks

DDoS attacks are more powerful than ever. There are a number of options for protecting your business. Act now because doing nothing is the expensive option that no business can afford. What is it? Distributed denial of service attacks, or DDoS attacks for short, overwhelm target websites with fake traffic to knock them offline, unless the organisation pays a ransom. How does it work? DDoS attacks were originally used by gamers to gain an advantage by slow- ing other players down. Hacktivists have used them to take down prominent websites to raise awareness of their causes. Criminals monetised the practice by demanding ransoms, often from online gambling operators or retailers, in exchange for being able to trade at busy times. DDoS attacks have increased in size over recent years. For example, in Sep- tember 2016 the website of security blogger Brian Krebs was hit by one of the biggest DDoS attacks recorded. It measured 620 gigabytes per second, nearly double the size of the largest previous attack. New DDoS variants gain their power from creating even bigger botnets — armies of hacked devices such as CCTV cameras, smart TVs and baby mon- itors — used to generate DDoS traffic. With attacks now being measured in terabytes rather than gigabytes or megabytes, DDoS attacks are a serious threat.

What's the impact? If you have a transactional website, you've got to be able to transact. Availabil- ity and reliability are critical, irrespective of what you sell. If customers can't reach your website, they're not your customers. This is particularly the case during the Covid-19 crisis, when your website may be the main, or only, sales channel to customers in lockdown. Aside from business disruption, DDoS attacks are often used as a smoke- screen for other nefarious activity. For example, data theft, ransomware at- tacks and malware activation. How can businesses protect themselves? There are a number of options for protecting your business from a DDoS attack. The level of risk and impact of an attack as well as your budget deter- mines what's right for your business.

- Host-supplied DDoS protection — your internet service provider or hosting company may offer DDoS protection as part of their package to you.

- On-premise hardware protection — offers real-time or near real-time DDoS detection, however this is often the most costly option.

- Cloud-based protection — an alternative to on-premise solutions which comes in a variety of flavours.

- Hybrid protection — best-of-both-worlds hybrid solutions combine on-premise hardware and cloud-based protection which can be tailored to your needs.

As well as technology solutions, consider insurance. It will not protect your business from attack, but purchasing insurance may help you recoup losses following an attack. Review the terms of your general business insurance policy and take out additional cyber-specific cover, if necessary.

How to fight back against SQL injection attacks

SQL injections have been a known vulnerability for more than a decade and defences exist. Make sure that your business deploys active defences against this popular but preventable attack vector. What is it? SQL or sequel is a programming language for managing and querying data held in databases. Dating originally from the early 1970s and developed by IBM, SQL is now widely used in various databases-driven websites. An SQL injection is an exploit where the attacker adds malicious code to an online form — typically a user login form — to gain access to the underlying database or change data. How does it work? SQL injection attacks allow criminals to disclose all the data on the system. This includes gaining access to internal databases that store sensitive pay- ment card data and/or customer data, such as usernames, passwords, ad- dresses and contact details. Criminals can destroy data or change data, for example void transactions, is- sue refunds or amend balances. They can make data unavailable. Or escalate their privileges to become administrators and take over the database server.

What's the impact? SQL injection attacks may have sig- nificant impact on the confidentiality, integrity and availability of data. Just how much depends on how much you rely on the application and data. The fallout of this is clearly business disruption and lost productivity if your website is offline or your business is otherwise unable to trade. Data breach- es create additional direct and indirect costs, such as the financial outlay of incident response, breach notification and fines. How can businesses protect them- selves? If your business is maintaining a robust level of security, then you have a good chance of fighting back against SQL injection attacks. Many of the policies and practices required for PCI DSS, the global data security standard adopted by the card schemes, are directly relevant to combatting such attacks. Here are our top five tips.

1. Protect your business from the internet Use a firewall as a buffer to prevent hackers and malware from accessing your e-commerce website, payment systems and/or card data. Ensure that hardware and software firewalls are configured correctly to prevent unauthorised access. Segregate your network, for example separate web and database servers so attackers cannot easily transverse your network.

2. Limit use of remote access

   Many remote access programmes are always on, or always available by default. This means vendors can access your systems remotely all the time — as can hackers. This is especially the case if vendors use commonly-known or default passwords for remote access. Reduce your risk by disabling remote access when not needed. And know how to enable such access if a vendor requests it.

3. Scan for vulnerabilities and fix issues Maintain a vulnerability manage- ment programme. This means doing regular vulnerability scans and acting on any risks. New vulner- abilities, bugs and exploits are being discovered daily. It's vital to ensure that your internet-facing systems are tested regularly to identify these new risks and address them as soon as possible.

4. Install security patches from vendors Software can have flaws that are discovered after release and can be exploited by criminals to steal customer and corporate data. Have a strong patching policy to deploy vendor-supplied security fixes as and when they become available. Some patches can be installed automatically.

5. Monitor and test networks Undertake appropriate proactive monitoring to discover attempted security breaches. Look on this as an early warning system to help prevent, detect and minimise the impact of a data compromise. Col- lecting logs and tracking user activ- ities are important for flagging any irregularities as well as for diagnosis when things go wrong.

How to fight back against credential stuffing

Credential stuffing is possible owing to the volume of large-scale data breaches in recent years. A layered approach of good password practices, restricted access and strong authentication is the most effective way to counter the practice. What is it? Credential stuffing is when attackers use usernames and passwords on one website to compromise accounts from other services. How does it work? Credential stuffing attacks are possible because many people reuse the same username and password combinations across multiple sites.

Criminals obtain credentials either from data breaches or from data dumps on underground forums. They then automate logins with credential pairs, using standard web automation tools. What's the impact? Media organisations, gaming companies and the entertainment industry are among the biggest targets of credential stuffing. However, conceivably any business where customers have to create or log into an account can be a target. Businesses that offer loyalty schemes, where customers can redeem points or credits against the purchase of future goods or services must also guard against the threat of fraud or unauthorised access. This is to protect their brand, reputation and bottom line.

How can businesses protect themselves? A number of good, basic countermeasures can be used to fight back against credential stuffing at a user and business level. Here are our top five tips.

1 Practice good password hygiene Encourage customers to devise unique passwords and login details for use on your site. At a corporate level, change default passwords for ap- plications and systems. If such passwords are readily available on the internet, they provide little to no security.

2 Use strong passwords Suggest to customers that they use strong passwords at least 12 char- acters long, but the longer the better. Advise them to mix letters, num- bers, cases and symbols. And to avoid sequences, repetition and actual names. Prompt for regular password changes. Advise customers not to share passwords across websites or with other people. The same advice applies to corporate systems.

3 Implement strong access control measures Segment your network to prevent so-call 'island-hopping' where attack- ers try to access sensitive data via third party suppliers.

4 Assign unique IDs Give a unique ID to each person with computer access within your business so they can be individually identified and verified. Monitor and track access to data and network resources.

5 Authenticate user Deploy strong or multi-factor authentication with customers and staff for access to accounts or systems. Using captchas on customer-facing login screens also helps to make automated attacks harder.

How to fight back against third-party supplier attacks

By collaborating and specialising, businesses gain from improved expertise, better products and services, faster speed to market, and cost or process efficiencies. However, no business today has direct control over every aspect of its operations, security or reputation, and must guard against third-party supplier attacks. What is it? Third-party supplier attacks are when criminals exploit a trusted third-party relationship as a stepping stone to attacking your business. How does it work? Any organisation is only as strong as its weakest link, which may be a third party. It may even be a so-called 'fourth party', a third party of one of its third parties. Indeed, in one high-profile case, attackers breached the security of a large US retailer via their air-conditioning vendor and stole the data of millions of credit and debit cards. Risks arise from the underlying outsourced activity, but also from involvement with third parties. Being interconnected, all organisations are affected by the culture and practices of others in their network.

Target faces massive bill over 2013 data breach Target agreed to pay Visa $67 million for a data breach in 2013. Criminals used stolen credentials from a third-party vendor to hack into Target's gateway server and access a customer service database. They installed malware to collect card data from around 40 million customers, and the personal contact details of around 70 million. Consumers and US state enforcement agencies also brought lawsuits against Target, resulting in further financial settlements.

What's the impact? The impact of a data security breach could be severe. This includes breach investigation costs, fines and negative publicity. There is also the impact of business disruption, recovery time, lost productivity and sales, if your website is offline or your business is otherwise unable to trade. How can businesses protect themselves? Businesses can implement various measures to protect themselves against third-party supplier attacks. Some relate to conducting thorough due diligence. Others relate to the processing, storage or transmission of sensitive cardholder data by third parties. Here are our top ten tips.

1 Determine roles and responsibilities so that it's clear who does what and that nothing falls between the cracks.

2 Maintain an inventory of third-party suppliers because knowing who they are is the first step to managing the risks that may arise.

3 Create a risk profile for each third party because the risks will differ according to the nature of the services provided, the mitigating controls etc. There's little value in spending €1,000 to protect a €1 risk. Implement access control to sensitive data on a 'need-to-know' basis.

4 Deploy isolation strategies (e.g. segmentation, intrusion prevention/detection) because not all third parties require access to card data.

5 Prevent easy remote access to your systems through trusted third parties. Limit the use of remote access to systems by third parties and ensure there are policies for disabling access when done.

6 Ensure third parties use unique logins and passwords, plus strong authentication. Make data useless to criminals when it is sent or stored using encryption and/or tokenisation technology.

7 Use strong passwords and ensure third parties have similar policies around making passwords difficult to guess, changing them regularly and not using default passwords.

8 Use anti-virus software because it's a no-brainer as part of a matrix of measures that you and any third parties can deploy to protect your systems.

9 Scan for vulnerabilities and fix issues in a timely manner as new security holes and bugs are discovered daily.

10 Ensure that third parties have an appropriately robust scanning and patching regime. Remember physical attack vectors, such as tampering with or swap- ping out payment terminals, can be as effective for criminals as digital ones. Remind your third parties of this and mitigate the risks accordingly.

How to fight back against terminal swap-out fraud

The most successful scams are often the most simple. Terminal swap-out fraud relies on nothing more than a convincing disguise and manner. Staff awareness is more than half the battle in fighting back, as is good practice around securing and inspecting terminals. What is it? Terminal swap-out fraud involves criminals who dress as maintenance staff. They come into stores and con staff by modifying or replacing termi- nals to capture card details. Once they have the magnetic stripe data or card PINs, criminals can make fake cards to withdraw money from ATMs. They can also sell the stolen card data. Or buy things with it to sell on for a profit. What's the impact? The impact of a data security breach could be severe. This includes breach investigation costs, fines and negative publicity, culminating in financial loss. How can businesses protect them- selves? If you operate retail stores, your staff are the first line of defence against criminal attackers. They are also your biggest vulnerability, because criminals set out to exploit human nature for their own advantage. Here are our top five tips to fight back against terminal swap-out fraud. 1. Challenge maintenance staff

Fraudsters look just like normal maintenance staff. It's not that hard to get hold of a high visibility jacket, boiler suit or tool box to look the part. Your front-line staff are there to be friendly and helpful to cus- tomers. And confidence tricksters take advantage of that to win their trust. Being aware of the scam is more than half the battle in defending against it. So tell your staff that routine maintenance is always booked in advance. If the maintenance staff are not down on the visitor list, they shouldn't be let in. Similarly, if they can't show valid ID, they shouldn't be let in. Genuine maintenance staff won't mind being asked for ID, being supervised or escorted whilst on the prem- ises. They're there to do a job, and won't mind your staff doing theirs.

2. Inspect terminals regularly

Rogue terminals look just like normal ones. So, examine your terminals regularly. Is there anything missing, such as screws or seals? Is there anything additional? Look for holes, scratches or stickers that could cover up tampering. Check the wiring, too. Are the wires the same colour and type as all the others? Be thorough. And compare your terminals against each other to spot any differences.

3. Secure terminals

Prevent your terminals from disappearing by securing them. Extra or spare terminals deployed at busier times should not be simply unplugged and stored under the counter. Treat them as you would your cash float. They're as valuable, if not more so. If it's not possible to physically secure your terminals, have reg- ular terminal weigh-ins to check nothing has been added, removed or changed.

4. Check for hidden cameras

It's not just missing or heavier terminals, though. Have extra terminals appeared? What about extra stuff on the counter? Leaflet boxes or charity tins? Anything that could hide a camera to record customers entering their PINs. Sometimes the fraud could be hiding in plain sight.

5. Monitor terminals locally and

remotely Know where your terminals are. This includes those in active ser- vice, in the storeroom under lock and key, out for repair or in tran- sit. It pays to check your terminal inventory regularly. Monitor your terminals remotely, too, with a terminal management system. If someone unplugs the terminal, you should get an alert.

How to fight back against Covid-19 scams

Criminals are unscrupulous opportunists. They've been quick to capitalise on the Coronavirus.

The UK's National Cyber Security Centre said that almost one-third of the total number of incidents it was called in to help with during 2020 were Covid-related. Meanwhile the number of cyber attacks hitting critical French businesses jumped fourfold in 2020, the French security group Thales confirmed. Cybercrime has shown a significant shift from individual and small business targets to major corporations, governments and critical infrastructure. In uncertain times, criminals are very good at putting new spins on old scams. Criminals still exploit the human factor, though. They prey on people's emotions, whether that's fear, desperation, generosity or greed. Being aware of their techniques to guard against them is half the battle in protecting yourself and your business.

Here are four familiar business scams re-booted for Covid times. 1.

Bank transfer scams

This is when criminals trick people into making bank transfers to accounts they control. It's also sometimes known as authorised push payment (APP) fraud. It cost UK businesses alone around £90 million in 2020, according to UK Finance.

Criminals are putting a Covid-19 spin on the fraud by asking businesses to transfer money to accounts supposedly at the Bank of England. We'd advise verifying all requests for transfers, bank or personal details with the organisation or individual making the request using established contact details. Do not reply to the e-mail or use the telephone numbers provided — they may be fake.

Consider introducing two-factor authentication for the corporate e-mail system to raise the bar against criminals. And be wary of what you post to social media, company websites and out-of-the-office messages. It's easy for fraudsters to create a targeted e-mail from such information.

2. Advance fee fraud

Victims are asked to pay a fee upfront before receiving stock, refunds, rebates etc. The scammer collects the money and disappears. Covid-19 related advance fee frauds include selling non-existent medical supplies, landlords purporting to offer retailers a rent deferral in return for a 10% downpayment, and fake offers of government assistance, grants and tax rebates.

Know the habits of your suppliers and business partners. Then you'll stand a better chance of spotting out-of-the-ordinary requests or sudden changes to business practices. If in doubt, double-check with a colleague even when working from home. Check sender e-mail addresses by hovering the mouse cursor over them. Also check they are spelt correctly and come from a corporate account rather than a free e-mail service, such as Gmail or Yahoo.

3. Tech support, software and fake anti-virus scams

With more employees now working from home, businesses face a higher risk of being defrauded by phishing and malware attacks. This is when criminals send e-mails that look like they come from trusted sources, such as the IT department. The e-mails claim that it's time to upgrade software or anti-virus protec- tion. But really, the criminals want recipients to click on links or open docu- ments that contain viruses or harvest login details or passwords. If you're not expecting the e-mail or don't know the sender, delete it without reading. Don't click on links or open attachments. If you're responsible for IT network security, consider e-mail filtering and network segmentation to protect against compromised devices and strong authentication for more secure areas.

4. Unusually large orders, new 'customers', fake creditors

We live, work and trade in unusual times. Nonetheless, be on your guard for new customers placing large repeat orders. Fake creditors are also making the most of Coronavirus cash flow issues. They contact business- es claiming that they are owed money or chasing late payment. They may even increase the pressure by threatening legal action, arrest or removal of goods to cover the value of the debt.

Conclusion

Awareness that these scams exist and how they work is half the battle in the fightback. Forewarned is forearmed. Human defences Your staff are one of the first lines of defence against many of the scams in this booklet. They are a business's eyes and ears on the ground, and can also function as its hive mind. However, your staff are also one of the biggest vulnerabilities, because they are often the target and are fallible. The definition of social engineering is is the art of exploiting human psychology, rather than technical hacking techniques, to gain access to systems, data or even physical terminals. Criminals are master manipulators. So, train your staff on how to counter the psychology of scams — the misdirection, time pressure and so on. Most staff have a personal mobile phone, comput- er or e-mail, so protecting their devices and data has become a life skill as much as a work compe- tence. Making training relevant to life outside work helps the content stick at work.

Technical defences It's unglamorous. It's unsung. But business-as-usu- al security is the bedrock of an effective technical defence. This includes best practices such as deploying firewalls, anti-virus and e-mail filtering. It involves patching systems and applications to fix known vulnerabilities, and doing so regularly. Restrict access to sensitive data and only store what your business needs. For the best protec- tion, make your data useless to criminals by using encryption and/or tokenisation. Don't give crimi- nals easy access to your systems and data, either through your staff or trusted third-party suppliers. Limit use of remote access and use strong authen- tication where appropriate. Lastly, the threat landscape is always changing. DDoS attacks have increased in strength. Ransom- ware has evolved to encompass double extortion. Criminals also put new spins on old scams as the Covid-19 crisis has shown. So, stay up to date with the latest trends. Good security is never finished. It's a continuous cycle of review, remediation and reporting.

How to reduce data security risk

Accepting card payment is a nec- essary part of running a custom- er-facing business. But storing, processing and transmitting card data comes with risks. Our hosted point to point encryption (P2PE) and tokenisation services help you take card payment without taking card data, thereby reducing your risk and PCI scope. Point to point encryption (P2PE) Encrypting data from the moment it enters your systems means you never see sensitive cardholder data in the clear. This helps reduce your risk in the event of a breach, the associated costs (e.g. lost revenue, damage to brand, reputation and trust), plus your PCI scope. PXP offers P2PE as a managed service for customers either as an application or as a full solution. Both have been tested by trained P2PE assessors against the PCI standard.

Tokenisation Tokenisation replaces sensitive card data with a token, which can be used across various front- and back-end systems instead of the real card data. PXP tokenisation works across channels, geographies and brands in a retail group. It can also be activated retrospectively on stored card details. This simplifies compliance with data security requirements, and also delivers operational, costs and marketing efficiencies. PXP's secure payment services help all types of business-es reduce their risk and are de-signed around 2 key principles: • Secure all sensitive consumer data - Reduce risk to merchant in case of a breach

PXP’s secure payment gateway helps merchants reduce their data security risk.