PROTECT YOUR BUSINESS AGAINST CRIME; pdf

1: Protecting your business against financial crime | HSBC UK

Four steps to protect your business against cybercrime Hacking is a lucrative business. Digital crime costs the world around $ billion a year and often occurs.

Cyber crime today is eye-wateringly big business. And that number could be just the tip of the iceberg, given that a high percentage of cyber crime still goes unreported. Different methods, same old crimes In many ways, much of this is nothing new. Cyber crime is effectively an evolution of traditional crimes â€" extortion, blackmail, fraud and so on â€" transported online. Modern cyber criminal organisations are fleet of foot, ingenious and highly professional in their approach â€" run by ruthless, rational entrepreneurs with great ingenuity and a determination to follow the money â€" which is now in cyberspace. There are three main types of cyber assault: Commoditised attacks, which are indiscriminate and deploy large scale attack software. Crypto coin mining using compromised IT systems has also become increasingly attractive, as criminals follow the market. Tailored attacks, identifying companies worth defrauding because they undertake regular payments to, for example, contractors and suppliers. These attacks scrape social media for contacts and connections and then send emails purporting to come from, say, a CEO and CFO, using the correct names and login details. There have been several high profile attacks recently, generally on softer targets in developing countries. Beating the criminals at their own game Given these increasingly pervasive risks, the climate has certainly never been more challenging. But there are a range of measures organisations can take to shore up their defences. How you can prepare: Adopt a holistic approach across your organisation, ensuring all the relevant separate security disciplines are joined up. Look at your fraud controls and how they monitor transactions and collect intelligence â€" and weigh up the right mix of detection and preventative techniques for your business. Step inside the mindset of the criminals to work out what they might want to target and how they would monetise it. Get the basics right - firewalls, anti-virus, patching, good passwords and other basic security solutions all still work well for many businesses as first line of defence. Ensure you have board level sign off and senior executive involvement across the organisation. Join forces with other businesses within the financial services industries, technology providers, law enforcement and Government to share information on the patterns of threats and current best practice. These issues need a coordinated community-based approach if the infrastructure used by organised criminal gangs is to be disrupted. Remember, transparency is essential. Firms face mandatory disclosure of any data breaches to information commissioners, shareholders and the wider public. Stay vigilant for the long haul: But in this complex game of cat and mouse, the more informed, fast and flexible your response, the better.

PROTECT YOUR BUSINESS AGAINST CRIME; pdf

2: Protect your business against crime | www.enganchecubano.com

Cyber crimes are increasing in number and intensity. Follow these five tips to make sure you're taking appropriate action to protect your business, employees and customers against cyber crimes: 1.

Your fears are well-founded considering the increasing cases of cyber crimes, with many entrepreneurs forced out of business due to this nefarious act. I want to give you some awesome and proven tips that will help you ward off cyber attacks from your business. Like I said, these tips are proven, which means that they work. Here are a few of those tips: Hype Up Your Security Consciousness This is an ironic statement, but your employees could be the biggest threat to your business. While they may not be directly involved in the crime, they are usually the door through which hackers have access to your information. For instance, when employees use poor passwords on their files or computers, they make their computers sitting ducks for hackers. Within a few minutes, the computers can be hacked. To prevent this, train your employees to make security their watchword. They can achieve this by using longer or more complex passwords. The rule of thumb is that passwords should be long and include uppercase and lowercase letters, numbers, and special characters. Hackers usually find such passwords difficult to break. In addition, passwords should never be reused for multiple accounts. Getting a security expert to train your staff just may be worth budgeting for as well. Protect Your Computers In addition to your migrating to cloud computing you need to give your computer systems the best protection available. Take these few steps to fortify them: It is advisable to install latest antivirus programs on your computers and to keep them regularly updated. They are specially designed to serve as the sentry to your network. Installing powerful firewalls on your systems gives cyber criminals a good reason to let you be. Software developers take the security of their users into consideration when developing Operating Systems. Latest versions are always equipped with the most potent protection against cyber attacks. Upgrading your Operating System then becomes an automatic protection for your business against invasion. Be Prepared For Invasion If you implement the suggestions above, your business is well protected and safe. However, you should always prepare for the big "What if? You should be prepared for such invasion by doing these: You should back up your files, data, and other resources that are the backbones of your business. You can always turn to the backed up files in case of data loss through the invasion. Restrict Access To Sensitive Information Making all the sensitive information about your business accessible to every Tom, Dick, and Harry is a good recipe for vulnerability. It is not wise to not know who accessed what and when. More so, if few people have access to such important information, it will reduce the chances of exposure to unauthorized individuals with evil intent. Restrict access to such sensitive information to the few people who have a business need to access it. Having a security expert on your payroll will cover up your inadequacies here. His job is to routinely check your systems for potential risks and prevent them. As a business expands in its operations, it creates greater loopholes for access. In case of intrusion, an expert, will use his expertise to mitigate the damages. Working with an expert means security gets the regular attention it requires. An experienced professional can identify risks and close security gaps before problems materialize. Compared to the cost of a data breach, hiring a security expert is a sound investment that will keep your business on the right track. As I earlier said, these tips are well-tested and have made the difference between victims to cyber attacks and those who have run a safe business for many years. Security investments are cardinal in the 21st century. So, fortify your business against such insidious attacks by implementing these tips. If you do this, your business will be safe, and you will be stress-free.

PROTECT YOUR BUSINESS AGAINST CRIME; pdf

3: 5 Ways to Prevent Cyber Crimes From Derailing Your Business | HuffPost

Understand What You're Up Against. Before taking any other action, work out how secure your business is currently. With a cyber security audit you'll get a clear idea of where your business is right now, while identifying any potential threats.

People can gather and share information. You can market and sell goods. You can communicate in real time with people on the other side of the world. Perhaps if I had the Internet available to me when I was attempting to complete essays and projects, it would have been a lot easier than trying to reference materials at the local library. But with good comes bad. The Internet can expose users to bullying, stalking and privacy violations. As well, storage and transfer of electronic data, including personal information like credit cards, has led to a wave of cyber crime. According to the U. Bureau of Justice, The vast majority of incidents involved the theft and fraudulent use of existing account information. These are staggering numbers. Of course business also use the Internet in the same capacity. Bills are paid online. Customer information is collected and stored. The following are a few suggestions for securing personal and business information online: Protect Your Accounts Choose strong passwords that incorporate letters, numbers and symbols. Most of us forget passwords, so keep a list in a safe, or invest in security software that can track passwords for various sites. You can access this with just one password you need to remember. This is a great idea for business too as many departments use different software and have varying accounts. As well, equip computers and mobile devices with security software. These alerts are often email notices. Make note of them and take action if you have received one. Be Wary As mentioned in the tip above, be wary when using free WiFi. This is where hackers can track your actions. If you can, use your own data service to do this. Read Your Bills Most of us, business too, pay their bills electronically. No matter what the type of payment, always review every change. Unexpected charges may be accidental, but they may also be evidence your data has been stolen. If you see an anomaly, report it right away. Take Action In , one-in-four consumers who received a letter informing them their data had been breached became the victim of identity fraud. Credit card numbers do remain the most popular item in a data breach, but other information can be more useful to fraudsters. If you receive a letter informing you of a breach, take steps to protect yourself like setting up account alerts or enrolling in an identity protection service. Data hacking can be an inside job too.

PROTECT YOUR BUSINESS AGAINST CRIME; pdf

4: How To Protect Your Business Against Cyber Crime - Prime Partners

10 Essential Ways to Protect Your Business Against Cyber Crime Cyber crime will cost businesses $2 trillion by and $8 trillion by 1 Costs can include damages resulting from theft of personal and financial data, stolen money, theft of intellectual property, fraud, lost productivity, forensic investigation, and reputational damages.

Share via Email Hackers may send emails disguised to look as if they come from a financial institution. The majority of attacks are phishing and spear phishing, where cybercriminals target individuals, rather than computer systems. A common method among hackers, for example, is to pose as a company boss in an email and persuade an employee to urgently wire company money to an account. Meanwhile, the more traditional form of cybercrime, infecting company equipment with malware, is still a problem. So how can small business owners and staff learn to spot â€" and stop â€" them? Put your questions to our experts from pm on Monday 21 November. Taking part is simple: Alternatively, tweet GdnSmallBiz with your questions, or email them to smallbusinessnetwork theguardian. Comments are currently open and we welcome questions in advance. Our panel James Snook is deputy director, cyber and government security directorate in the Cabinet Office. He has held a number of roles across the cabinet office and HM Treasury. His career has focused on national security, and cyber security, especially, in recent years. David Jeffrey is product director, fraud and security at Barclaycard payment solutions. He is responsible for developing products and services, aimed to protect customers against fraud and payment security threats. IASME was closely involved in the development of cyber essentials, a basic information security standard developed with the government. Randall is also the founder of The Friendly Nerd, a startup specialising in cyber and data security training. Jenny Radcliffe is an independent security consultant and trainer who specialises in social engineering, in which people, rather than IT systems, are the target of cyber criminals. She trains businesses in how to protect themselves, and is the host of The Human Factor podcast. Paula Barrett is head of data privacy and partner at Eversheds law firm. She has been advising on the legal aspects of data protection and cyber security for over 20 years. Cindy Ng is a security and privacy expert at Varonis , an American software company that offers software solutions to protect data from insider threats and cyberattacks. Sign up to become a member of the Guardian Small Business Network here for more advice, insight and best practice direct to your inbox.

PROTECT YOUR BUSINESS AGAINST CRIME; pdf

5: How to Protect Your Business Against Cyber Crime

This blog offers more advice on what to look out for and digs deeper into your options: 4 Ways to Safeguard and Protect Your Small Business Data. Use a Dedicated Computer for Banking This is a great idea from Forbes magazine's 5 Ways Small Businesses Can Protect Against Cybercrime.

Each business has its own web of connections, often stretching across the globe. Hacking is a lucrative business. Taking the offensive - Working together to disrupt digital crime Image: BT and KPMG As the pace and variety of attacks increase, you need to keep ahead and there are four things you should be thinking about: Is the board on board? They need to be constantly thinking about the worst case scenario: How badly would your business be damaged if one individual were bribed or blackmailed? What are all the possible ways someone could attack? Board members with backgrounds in digital security and risk management can help the board, and even senior management, better understand the issues and more effectively communicate with the security team. Other C-level roles will also need to evolve. The chief information security officer CISO , for example, will need to be elevated from a traditional IT-focused role to one with direct accountability to the CEO and regular reporting to the board. Chief information officers CIOs will need to factor risk mitigation into every step the organization takes on its digital journey. Is security part of your culture? Give them responsibility, and encourage them to speak up. For example, a recruiter can consider how much a planted employee could steal. They might then be proactive and help ensure you have the right vetting processes in place. Have you separated your data? The trick is to make sure you have layers between your systems. You want to make sure your most valuable information is hidden â€” even from your own employees. Do the same with your data.

PROTECT YOUR BUSINESS AGAINST CRIME; pdf

6: How to Protect Your E-commerce Business from Cyber Attacks

Therefore, it makes sense to take the right security measures to protect your business from crime. Minimise crime opportunities The security measures you should take will depend on factors such as your business location, the type of goods you sell, the type of equipment you use, your trading hours, whether you handle cash, and the staff you employ.

Whether small, medium or large, every business is, sadly, at the mercy of hackers who will exploit every opportunity they get to breach sensitive data and use it for their ulterior motives â€" mainly, to make an easy buck. The number of data breaches increased by These attacks have resulted in massive financial losses to the point that some businesses had to permanently close their doors. Ways to Protect Your Online Business against Hackers When it comes to protecting your business against cyber attacks, there is a myriad of online solutions that can come to your aid during the most desperate of times. For starters, to better protect your business, make sure your employees are educated on the most common types of cyber attacks. Here are some ways you can protect your online brand from falling victim to cyber attacks. Use a Secure E-commerce Platform Host your e-commerce website on a platform that supports sophisticated object-orientated programming languages. The main reasons behind the popularity of this plug-in include low-cost, easy setup and high security. With strong SSL, no third-party would be able to make any sense of it due to the encryption. Beware of Social Engineering Scams Social engineering involves emails or any other sort of online communication that invokes urgency, fear, or similar emotion in the victim, tricking them to promptly reveal sensitive information, click a malicious link, or open a malicious file. About 12 percent of all recipients went on to click the malicious attachment or links that enabled the hacker to successfully attack a business. Try asking your customers to add special characters, mixed numbers and symbols in the passwords the use to make accounts on your website. Motivate them to use longer and complex passwords. Complex and longer logins will make the job of hackers that much more difficult. Layer Your E-commerce Security Layering your security is one of the best ways to keep your online business safe against cyber attacks. Start with firewalls, since they are essential for stopping attackers before they can breach your network and gain access to the sensitive information. You can then add extra layers of security to your website and applications, such as contact forms, login boxes and search queries. It ensures that your e-commerce portal is protected against application-level attacks, such as SQL injections and XSS. Follow him on Twitter anasbaigdm. The opinions expressed in this guest author article are solely those of the contributor, and do not necessarily reflect those of Tripwire, Inc.

7: 4 steps to protect your business against cybercrime | World Economic Forum

The days where cyber-security was something that small business could afford to neglect are long gone. Today, the threat of cyber-attacks is simply too large, imminent, and dangerous to ignore. Of.

8: Cybercrime: how to protect your business | Guardian Small Business Network | The Guardian

COMMERCIAL CRIME INSURANCE | CLAIMS SCENARIOS Help protect your business against employee theft with commercial crime coverage. Employee theft costs businesses billions of dollars each year.

9: Mind games: Protect your business against cyber crime | KPMG | UK

Protect your business from organized cyber crime rings that may include the following players: Programmers: These skilled tech pros write and code the viruses that infect a business's computer.

PROTECT YOUR BUSINESS AGAINST CRIME; pdf

Forest Growth Responses to the Pollution Climate of the 21st My Mothers Autumn Paleotethysides in West Yunnan and Sichuan, China Sample sop for mechanical engineering Hunting the Dinosaurs and Other Prehistoric Animals (The New Dinosaur Library) Kentucky survival (HRW basic education) Capital financing Alice Paul : a tireless fighter Walking into the Lyons den Gleanings on the Magdalen Islands A New Hope (Star Wars: Infinities) ARM system architecture Marcel Duchamp: The Bride stripped bare by her bachelors, even. Song of the Wanderer (The Unicorn Chronicles, Book 2) Spirit of the Prairie Dont slam the door! Nag Hammadi Texts and the Bible Economic development by todaro and smith 8th edition Decorative Art 50s (Decorative Arts Series) Geotechnical earthquake engineering nptel V. 1. Invertebrates and Nonmammalian vertebrates. Early monastic Buddhism. Paleoaltimetry from stable isotope compositions of fossils Matthew J. Kohn, David L. Dettman Washington post march sheet music The great neighborhood book Happy Snappy Jolly Jungle (Happy Snappy Books) Romance of Rosy Ridge English to Odawa dictionary and grammar with translations of Odawa legends from Odawa to English plus ora Thinkers guide to the art of socratic questioning Quest for being, and other studies in naturalism and humanism. Legends of the Field Fast fun for ages 11-13 Dissemination of grant findings. Modern casserole cookery Samurai (Time Soldiers) Napoleon and his wars. Equilibrium activity diagrams Be Kind to Your Mother (Earth : As Original Play) Recent trends in green chemistry Oxford Advanced Learners Encyclopedic Dictionary