HISCOX

The A-Z of cyber security

For small businesses

Hiscox cyber guide – A-Z foreword

Did you know that the total annual cost of cybercrime against small businesses, in 2014-2015 was around £5.26 billion[1]? This may seem surprising, but perhaps not when we consider that most information now exists as some form of digital asset, stored in places that go far beyond the four walls of the business it belongs to. This means that most data is potentially accessible to anyone in a given organisation, plus suppliers, partners and any number of external people with the right tools and knowledge.

As systems age and become more interconnected through the internet, the number of security vulnerabilities is on the rise, with high profile breaches hitting the headlines regularly. This, along with the rapidly evolving nature of cyber threats, has put cyber security at the top of the agenda for many small business owners.

CGI's recent study on cyber security in the boardroom conducted with the Centre for Economic and Business Research uncovered some of the key challenges that senior business executives face when it comes to tackling cybercrime. The findings revealed that 38% of the board-level executives asked expected their organisation to suffer a breach within the next twelve months. In dealing with cyber security, almost 28% of boardrooms in the UK's key sectors - telecoms, utilities, finance and retail - still view cyber security as an IT issue, instead of the company-wide risk that it is. And only 35% of the surveyed business leaders believed that their board members are equipped with the necessary levels of cyber security expertise.

While the majority of UK businesses are planning to increase IT spend on cyber security and focus more efforts on reducing cyber risk, the management and control of such risks at board level is still ambiguous.

To be able to effectively manage cyber security risk, small business owners should be striving to educate themselves. They need to understand the language of security in order to spot cyber-attacks and make sure that the right actions are being taken.

This A-Z outlines some of the common terms used in the topic of cyber security, as well as related expert advice, providing the first step for small business owners who want to better protect themselves. It's an essential companion to those who want to take action to address the challenges that cybercrime presents as we move into a future where it's all too present.

Andrew Rogoyski
Vice-President of Cyber Security at CGI
www.cgi-group.co.uk

[1] *http://www.fsb.org.uk/docs/default-source/fsb-org-uk/fsb-cyber-resilience-report-2016.pdf?sfvrsn=0*

List of influencers

Sam Pudwell, IT Pro Portal

www.itproportal.com

Sam Pudwell is Production Editor at ITProPortal, a well-established B2B technology publication aimed at IT professionals. With a focus on the enterprise side of the industry, ITProPortal covers all of the key areas in technology, from key business trends such as mobile and cloud to public sector news and analysis. Whilst tending to focus on cyber security, Sam also writes about cloud computing, digital transformation, big data and covers general industry news.

Adam Shepherd, IT Pro UK

www.itpro.co.uk

Adam Shepherd is a staff writer for IT Pro and Cloud Pro, and has previously written for PC Pro, PC Advisor and GamesRadar. He covers both business and consumer technology, but has a particular love for all things gaming, and is paying special attention to the emerging VR market.

Eleanor Burns, Computer Business Review

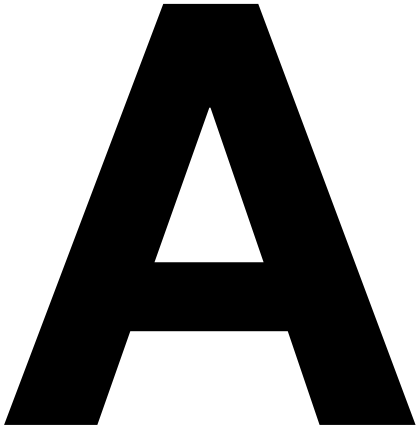
www.cbronline.com

Ellie Burns is the News Editor for Computer Business Review, managing a news desk reporting on a host of business technology issues – from big data, to cloud and IoT. Previously, she held editor positions at Actuarial Post, a financial trade publication, and Electronic Specifier, a technology trade magazine. Beginning her journalism career as a freelance reporter in Japan, she has also previously edited children's books and advised on a number of sites and blogs.

Andrew Rogoyski, CGI

www.cgi-group.co.uk/systems-integration-services/cyber-security

Andrew brings a significant breadth and depth of experience in cyber security having worked across technology providers, UK government and academia. Andrew joins CGI from an extended secondment to the Cabinet Office's Office of Cyber Security and Information Assurance (OCSIA), latterly supporting UKTI in the promotion of the UK's cyber companies overseas, following a long career working for a variety of ICT and technology companies. Andrew currently chairs TechUK's Cyber Security group which he created in 2008.



Threat name

Adware

Adware refers to any advertising banners displayed within software applications. Extra code is written into the software by its author, which serves up the ads as the application is running.

Description

One of the most high-profile cyber security breaches involving adware came in 2015 when the multi-national technology company, Lenovo was found to be pre-installing a type of adware that became known as 'Superfish.' The adware issued and installed its own security certificates, enabling it to intercept any information sent and received by the user's device, putting them at increased risk.

Lenovo was forced to release a software update and a tutorial explaining how to remove the Superfish programme and the scandal seriously harmed the company's reputation.

Adware has also been found in the Google Play Store in the past, with one example being Android.Spy.510, which worked by displaying ads on top of normal applications.

How does it work?

Once installed on the device, adware automatically shows unwanted ads in order to generate revenue for the brand, as well as collecting marketing data and other information without the user's knowledge. What is tricky with adware is that it usually goes unprotected, so can be very lucrative for attackers.

Not all adware is bad, but some variations will undermine your security settings and display ads that can later be exploited by more dangerous hackers. Infection can have various effects depending on the type of adware, but some of the most common include slowing down your device, continuous pop-ups (which are as annoying as they sound) and constantly tracking your activities online, known as 'spying'.

Protection tips

The most common ways to pick-up adware are by downloading freeware or shareware that has it built-in or by visiting an infected website. The first steps for protecting yourself should be to avoid downloading programmes from unfamiliar websites, likewise with software unless it's absolutely necessary.

Aside from that, targeted adware removal tools can be bought from most security software vendors and make sure you scan your devices regularly for any potential viruses.

B

Threat name

Backdoor Trojan

Backdoor Trojans enable hackers to take control of someone's computer via the internet without their permission.

Description

Trojan viruses have had several high-profile successes in recent years, with Skype and Readers Digest being two notable examples. Both Windows and Mac systems have fallen victim to Trojan attacks, and hackers will often let them lay dormant for many years before bringing them back to the surface.

Some recent strains include BackDoor.TeamViewer.49 (which disguises itself as an Adobe Flash Player update), Bayrob (first discovered in 2007 with the goal of stealing sensitive information) and Pinkslipbot (able to steal banking details, email passwords, and digital certificates).

How does it work?

Trojan malware is often disguised as legitimate software and enables hackers to do things like spy on you, steal your personal data or access and control your system. Backdoor Trojans specifically give cyber criminals remote access to the infected computer, enabling them to do anything they want - such as sending and receiving files, running programmes or rebooting the computer – as if they were the system's administrator.

Backdoor Trojans also often contain added threats such as keystroke logging (where a device or piece of software records all actions made on a keyboard), screenshot capture and file encryption, all of which combine to form a serious security threat that's nearly impossible to detect.

They're often used to unite a group of computers to form something known as a 'botnet' or 'zombie network' that can be exploited for criminal means. Backdoor Trojans often gain access to a computer through social engineering (see S) techniques where users are persuaded to click on a link in a spam email or visit a compromised website.

Protection tips

The best way to protect yourself against Backdoor Trojans and other strains of Trojan malware is to keep all the computers in your network up to date with the latest patches, which are fixes for known system vulnerabilities. You should also install effective antivirus and anti-spam software. Also, always avoid opening emails that look like spam. When trying to spot these, look out for things like poor grammar and spelling mistakes and threatening or urgent language, as these are clear signs of illegitimacy. If you think you've opened up a spam email, don't open any attachments or click on any links to external websites.

C

Threat name

Chain letters

Chain letters refer to emails that urge the recipient to send it on to other people.

Description

Most people can probably remember seeing chain letters circulating in their email inbox or on social media. They're usually asking for charity donations or describing some pointless number-crunching game before urging the recipient to send it on to as many other people as possible. While they can seem like just a bit of fun, chain letters can actually pose some serious security risks.

In one of the most famous examples in the early 2000s it stated that Bill Gates was sharing his fortune and that you would receive $245 for sending the letter on. It even cites a fake attorney called Pearlas Sandborn. As ridiculous as the letter sounds, it's surprising just how many people tend to fall for scams such as this one.

How does it work?

Most chain letters will seek to play on the emotions of the recipient and are usually very well-written and convincing. They'll ask you to donate money, usually to a child in need, persuade you to download software by issuing false warnings about a new virus or try to lure you in with get-rich-quick pyramid schemes.

Cyber criminals will look to play the odds with chain letters by sending them to as many people as possible. Thanks to the rise of social media, the increasing number of mobile users and the continued proliferation of the internet in general, it's now relatively easy for hackers to get these letters out to hundreds of thousands of people at once.

The main privacy and security threats posed by chain letters are email spam, online fraud through fake donations, identity theft via phishing techniques and virus infections delivered through malicious attachments or links.

Protection tips

The best way to protect yourself against chain letters is to immediately delete any messages that ask you to send them on to other people. Always avoid clicking on attachments and links to other websites and don't hand over any personal information unless you know it's genuine and are absolutely sure that you know where you are clicking through to.

Finally, make sure all the computers in your network have effective antivirus and anti-spam software installed and warn your employees about the dangers of chain letters.

D

Threat name

Data theft

Data theft refers to the theft of confidential information by cyber criminals.

Description

Data theft is one of the hottest topics in cyber security at the moment and is an issue affecting businesses of all sizes, in all industries.

Several high-profile companies have fallen victim to data breaches in the last few months, thrusting the issue into the spotlight for businesses, governments and consumers alike. Just recently, Acer suffered a data breach through its website and before that the likes of Tumblr, Twitter and Ofcom have all had customers' personal information stolen by cyber criminals.

In fact, the news of yet another data breach has become an almost daily occurrence and, with significant financial rewards when hackers get hold of this data, it's a trend that is unlikely to slow down anytime soon.

How does it work?

There are a variety of methods hackers can use to gain access to company information. Humans are generally known to be the weakest link in a business's defences, so hackers frequently target employees with phishing emails and use social engineering (see S) techniques to get hold of vital information such as passwords and login details.

Various strains of malware and viruses can also be introduced to business networks through methods such as malvertising (when malicious ads are injected into legitimate online advertising networks), malicious email attachments or by exploiting vulnerabilities in the network. Once inside, hackers can remain hidden for a long time, slowly building up a blueprint of the system and collecting the details they need to access private data.

Protection tips

The first step in protecting your data is to make sure all your firewalls and security systems are up-to-date and that there are no glaring vulnerabilities for cyber criminals to exploit. Next, make sure all your important data is encrypted. This will render it useless even if hackers do manage to steal it.

It's also worth monitoring outgoing emails that have data attached to see the type of attachments and where the email is going, as hackers will often programme malware to send information back to base in small amounts.

Finally, make sure all your employees are aware of the threats and train them to be able to spot criminal techniques. By knowing how to spot phishing emails and understanding the dangers of giving out confidential information, your employees can be a great asset to your security armoury.

E

Threat name

Extortion hacks

An extortion hack is when data is stolen with the specific aim of blackmailing the victim.

Description

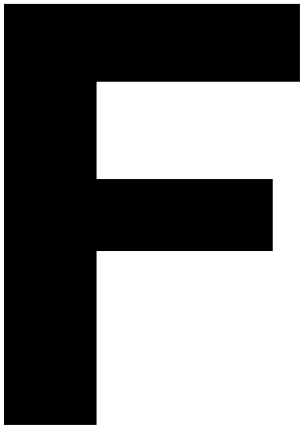
In an extortion hack, the hacker threatens to release sensitive company data unless the business pays up or meets a demand. Back in 2014, Sony publicly fell victim to an extortion hack, when a group that called itself the 'Guardians of Peace' (GOP), leaked confidential data from Sony Pictures Entertainment. It contained information about employees, including emails between them and copies of then unreleased Sony films.

How does it work?

Hackers use a variety of methods to steal company information. They often target employees – known as the weakest link in a business's defences – with social engineering tactics (See S), and use the passwords and confidential details they gather to log into the business network. And there are various strains of malware viruses (See D), distributed through spam emails or by exploiting vulnerabilities in the network. Once they've gained access, hackers can build-up a blueprint of the system and steal the details they need to collect private data.

Protection tips

The key to avoid falling victim to an extortion hack is to make sure your data is protected. See D for Data Theft.



Threat name

Fake anti-virus malware

Fake anti-virus malware is a particular type of malicious program that aims to extort money from people. This is achieved through claiming that the victim's device is infected and that they need to buy 'rogue' security software to combat the issue.

Description

Fake anti-virus malware is one of the most persistent threats on the Internet today. It's often called 'scareware' as it displays alarming messages to the user, encouraging them to take action as a result of the message. This kind of malware has the ability to take control of your device and disable your original security software making it even harder to remove.

How does it work?

Fake anti-virus malware often appears as pop-ups when browsing the Internet. The pop-ups often warn the user that their device may be infected, prompting them to download new software that is available at a link provided. Clicking on the link is likely to install further, more serious malware, onto the computer system. The pop-ups may simply redirect the user to a website that sells fake antivirus software and asks the user to enter their credit card details.

Protection tips

The first step in protecting yourself from fake anti-virus malware is to never click on a pop-up window. Always use the 'force quit' or 'Control + Alt + Delete' function to close the window instead. If you have any concerns about your device's safety you can run a scan using legitimate security software. In general, it's important to keep your devices updated with the latest security software to protect yourself from such online threats.

G

Threat name

General Data Protection Regulation (GDPR)

GDPR harmonises data protection law across Europe, increasing the responsibilities and levels of sanctions imposed on organisations that mishandle sensitive personal data.

Description

The GDPR was agreed by Europe in December 2015 and adopted on 27 April 2016, although the law comes into full force in May 2018, businesses should begin preparing now. GDPR replaces existing data protection regulation, originally developed as part of European Regulations in 1995.

How does it work?

Coupled with the recent agreement of the Network Information Security Directive (NISD), there's now a powerful force for change in cyber security being driven through Europe. The threat of a fine, which could be as much as 4% of global revenue, should drive some real behavioural changes in terms of how organisations secure sensitive data. Because GDPR will apply to any firm operating in Europe, it will have a profound effect on data protection and security across the globe.

The GDPR means that IP addresses, cookies and radio frequency identification (RFID) tags, as well as medical data, including genetic data are now treated as sensitive personal info. This could prove challenging to some businesses.

The GDPR also means the 'right to be forgotten' is now encapsulated by regulation. So customers now have the right to ask a business removes all data and personal records relating to them from their databases and systems and companies must act on the request.

H

Threat name

Honeypot

Honeypot is an advanced cyber defence process where a computer system is set up as a decoy to lure cyber attackers. The system is used to detect, deflect and study strategies that are used to access information systems.

Description

A honeypot needs a computer, often represented as a network of virtual machines, together with applications and data that are able to simulate the behaviour of real systems that appear to be part of a network. In reality, such a system is carefully isolated and very closely monitored.

How does it work?

Honeypots can provide a close analysis of hacker activity and how attackers are able to develop and progress, providing organisations with the knowledge of how to better protect their systems. Honeypots can also be used as network detection systems, providing a form of alarm when an intruder penetrates the system. They're purposefully designed to appear real and contain information of interest to attract and occupy hackers.

Threat name

Incident response

An incident response is an organised approach to addressing and managing the aftermath of a security breach or attack.

Description

The goal of an incident response is to handle a volatile security-breach situation in a way that reduces any further damage, recovery time and costs. An incident may be declared when it becomes obvious that a system has suffered data loss or operational disruption. The incident response plan includes a policy that defines what constitutes an incident and provides a step-by-step process that should be followed when an incident happens.

How does it work?

The incident response team is typically made up of people from the IT, Security, Legal, Human Resources and the Public Relations departments. Their role is to establish if a security incident has taken place, and then to contain the attack to prevent it from spreading any further. Once contained, the team focuses on finding the root cause of the problem and eradicating the issue. Lastly, the team will aim to restore the systems to operational use.

Incidents may come to light as a result of pre-emptive advanced investigation techniques, so-called ‘hunting’ for hacking attacks. As well as when confidential information is simply found outside of the organisation or when systems are disrupted by attackers.

Protection tips

One way you can protect your business from online attacks is to educate all staff members on the security measures within the company. And it’s wise to have a backup strategy in place. For other relevant protection tips visit ‘S’ (social engineering), ‘P’ (passwords) and ‘D’ (data theft).

J

Threat name

John Brennan

In 2015, a high-school student hacked into the AOL email account of the director of the CIA.

Description

The method the hacker and his accomplices used is often referred to as ‘social engineering’ (see S), which is when a hacker relies on human interaction to gain access to confidential data. The hacker did a reverse look-up of Brennan’s phone number to discover that he was a customer of the Verizon mobile network. Then he or one of his accomplices rang the company posing as a Verizon technician and asked for details about Brennan’s account. Providing a completely fabricated ‘Vcode’ (a Verizon employee number), the hackers were given enough of Brennan’s personal details to successfully log into his AOL account, gaining access to dozens of highly confidential emails.

How does it work?

There are numerous types of social engineering attacks that can be used for many different cybercrime activities. In this instance, the attack relied on a person giving away confidential information to someone they believed to be legitimate.

One type of technique is called baiting, where an infected device like a USB is left in an easy-to-find place. The person who stumbles the USB loads it onto their computer (out of curiosity) and unintentionally installs malware or a virus. See ‘S’ for more information.

Protection tips

Businesses should give all employees training and guidance in regards to social engineering. See ‘S’ (social engineering).

K

Threat name

Keystroke logging

Keystroke logging or ‘keylogging’ refers to the process of recording all keystrokes on a computer keyboard. A keylogger is the software or hardware device that logs the strokes.

Description

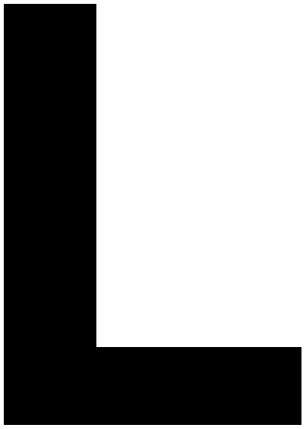
Keystroke logging is a common method used by hackers, and involves recording everything someone types on their keyboard with the aim of stealing confidential information. Once they’ve installed the software or hardware needed to do this, hackers have completely free access to information such as usernames, passwords and bank details.

How does it work?

Keyloggers are generally installed by malware (see M), but can also be installed in the form of hardware by, for example, disgruntled employees, jealous spouses or protective parents. These hardware keyloggers come in the form of a USB stick or a device that can be plugged into the keyboard. They have an advantage over software because they can start recording keystrokes as soon as the computer is turned on, meaning they can capture initial login details.

Protection tips

To detect hardware keyloggers check all the devices are physically connected to your computer and make sure you know why each one is there. It is also worth noting that Keylogger software runs invisibly in the background, as it’s another form of malware. For protection tips, go to ‘M’ (malware).



Threat name

LastPass

In 2015, a security researcher released a tool that was able to steal confidential data from the master password manager, LastPass.

Description

While stored passwords weren't stolen during this hack, the hackers gained access to LastPass customers' email addresses, password reminders and authentication hashes. Although LastPass claimed to believe that no user accounts were accessed in this attack, they did advise all customers to change their master passwords.

How does it work?

Like most password managers, LastPass stored the master passwords of its customers in the cloud in an encrypted vault. The vault was protected by a single username and password. This attack relied on a user visiting a malicious website, which then detected if the browser was using LastPass. Once detected, it mimicked a LastPass notification, remotely logged the user out and then asked for their password and two-factor authentication key. This method is known as 'phishing' (see S and P).

Protection tips

For password protection tips visit P (passwords) and S (social engineering).

M

Threat name

Malware

Malware or, ‘malicious software’, is a programme or piece of code implanted into a computer system for criminal purposes. It’s also known as a computer virus.

Description

Malware comes in many forms, from Backdoor Trojans (see B) to ransomware (see R). When malware first appeared in the 1980s and 1990s, it was often used for vandalism, destroying computers or displaying mocking messages.

Today, however, it’s much more sinister and is frequently used for profit by gangs of cyber criminals. Thanks to the rise of the internet and anonymous dark web marketplaces, hackers can buy and sell pre-made malware, ready to implant in victims’ computers.

The goal of most malware is to make its creators a profit through tactics such as extorting the victim for money, or harvesting their personal information, usernames and passwords and selling them online.

How does it work?

Malware can be delivered in many different ways. One of the most common is by code embedded in email attachments. Hackers will send the victim an email to try to trick them into opening the included file. This is known as ‘phishing’ - for more information go to ‘S’ (software).

It can also be installed via a ‘drive-by download’, where the victim is fooled into visiting a website containing malware. These websites are often constructed to look like websites you know and trust, such as social networks or banking sites. Packaging the malware inside another file or piece of software which is downloaded by the target is another commonly delivered method. Browser toolbars, screensavers, and illegal music and movie downloads have all been popular examples of this tactic.

Protection tips

For password protection tips visit P (passwords) and S (social engineering).

N

Threat name

Non-compliance

Non-compliance is a failure to abide by government rules and regulations - in this case, those relating to cybersecurity and data privacy.

Description

Data protection regulation is designed to make sure that businesses take proper care when handling customers' data and details, ensuring that it doesn't fall into the hands of hackers or cyber criminals. This includes setting out minimum cybersecurity standards that businesses have to meet, establishing procedures and practices for how to respond if there's a data breach, and fining businesses who are found to be non-compliant.

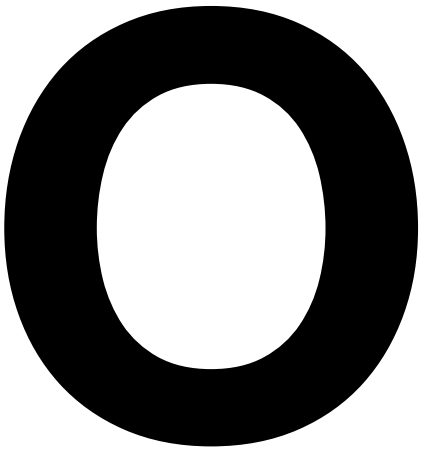
How does it work?

One example is the General Data Protection Regulations, which is a new set of regulations that governs how companies handle the data of EU citizens, due to come into effect in May 2018. The rules apply to anyone who stores or processes data of EU citizens - including small businesses. They include regulations that require companies to inform the authorities of a data breach within 72 hours of it happening, alongside other measures (See D). The maximum fine for non-compliance with this legislation is set at 4% of a company's global revenue.

Protection tips

Legislation - particularly dense and wide-ranging EU legislation - can often be difficult to get your head around, but you have to make sure that you know, and are compliant with, all the regulations relating to your specific business or field.

There many official resources online to help you with this, which include support and guidance on which laws apply to you and how you can comply. There are also professional compliance experts who you can hire to make sure you don't run into trouble with any legal grey areas.



Threat name

Online hackers

Online hackers are people who may attempt to break into, destroy or vandalise your computer or IT network.

Description

There are numerous different breeds of hacker. Some pick their targets at random for their own amusement, some operate based on political or ideological beliefs, and some are in it for financial gain. Each hacker is different and has their own personal level of skill. Even within hacking groups, the actions and responses of members can vary wildly. Not all hackers are bad, either - some are 'white hat' hackers, who disclose any security flaws they find to their victims.

The main thing they have in common, is that your business is a potential target for all of them. There's no such thing as a business that's too small to hack, and your customer data is always valuable on the black market.

How does it work?

There are many techniques that hackers can use to attack your systems, and more are being invented every day. These include many of the active threats on this list, such as phishing (see P), malware (see M), exploit kits (a type of malicious toolkit used to exploit security holes found in software applications).

Once they're inside your network, a hacker can do many things. They can snoop through your files, they can steal sensitive databases and information, or they can immediately set about destroying or defacing your system. Alternatively, you may not know you've been hacked at all. An intruder can very easily exist inside your network for weeks, if not months, waiting for the right time to take action. In some cases, hackers have bided their time for years before revealing themselves.

Protection tips

Hackers have access to a vast toolkit, so you need to protect yourself against as much of it as possible. Follow best security practices, such as using strong passwords, not downloading questionable files and staying away from untrustworthy websites. Your best weapon is knowledge. For hackers, an uninformed target is an easy target. Try and keep as up to date with cybersecurity news as possible, looking out for any trends or patterns of attack that could be used against your business.

P

Threat name

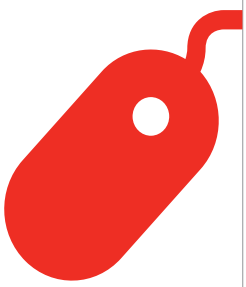
Passwords

Passwords act as a digital key, giving access to your files, systems and services while making sure that you are who you say you are.

Description

Thanks to smartphones and social networks, passwords are now an integral part of our daily lives, but it can be easy to forget how important they are. Passwords are often the only barrier to keep our data and devices from falling into the hands of internet cyber criminals, which is why it's so vital to make sure they're secure.

With access to just one of your passwords, a talented hacker can find their way into many more of your online accounts, gaining access to personal and private information.



How does it work?

The strength of a password is based on how difficult it is to guess. This is why passwords like 'password', 'football', 'qwerty' and '12345' are bad passwords - they're all very predictable. Unfortunately, they're also the most common. One method of stealing passwords is called 'social engineering' (see S), where hackers rely on people giving out their passwords on the phone or in person. Another is called 'phishing', where hackers will use malware (see M) to throw up fake messages on a user's computer claiming they need to re-login to a site such as Facebook, or their bank account.

Protection tips

A good password should be difficult to guess not only by a hacker, but also by the software tools they use. These programmes run through a vast number of potential passwords in quick succession, trying common words and phrases, as well as various permutations of them.

Passwords should also be unique to each individual device, site or service for obvious reasons. If you reuse a password multiple times, any hacker that obtains that password will have instant access to different sources of your data.

Q

Threat name

Quarantine

Quarantine is a function performed by antivirus software, where a file showing signs of infection is isolated on a computer's hard disk. This isolation makes sure that the file, if infected, can't harm or further infect the host computer.

Description

Quarantine is essentially special computer storage for suspicious objects potentially infected with a virus. While in quarantine, the suspicious file will be unable to run and will remain like this until the user decides to delete, fix or release the file from quarantine.

How does it work?

Antivirus software, either pre-installed or installed by the user, doesn't automatically delete every file it suspects of being infected. This is why quarantine was introduced - the deletion of files suspected of being infected may lead to unaffected files – ones that are important to the user – being deleted by accident.

When a computer's antivirus software identifies a suspicious file, a user is normally given three options: *clean, quarantine and delete*.

The clean option can be used to remove the infection from the file. However, this only relates to viruses where a legitimate file has been infected with malicious, normally viral, code. Threats like worms and Trojans cannot be 'cleaned' as these are not infections - the entire file is either a worm or Trojan. The delete option completely removes the file from the system, which leaves quarantine as the middle ground between clean and delete.

Protection tips

When faced with a suspicious file, always start with the 'clean' option. If the antivirus reports that the clean was unsuccessful, then put the file straight into quarantine. In quarantine, the file is safe and won't damage the rest of your computer. If you are 100% sure that it's not a legitimate file, or if the antivirus recommends it, delete the file. Remember – once deleted, there's normally no way to get these files back. If you're unsure about a file, leave it in quarantine and regularly update your antivirus software. With each update, run a scan and check if the file is still identified as a threat.

R

Threat name

Ransomware

Ransomware is a type of malware that allows hackers to hold a user to ransom by restricting access to an infected computer system.

Description

Ransomware has become a widespread, constantly evolving, threat to cyber security – with some experts describing it as an epidemic. In just a year, between April 2015 and March 2016, the total number of users hit by ransomware increased by 17.7% to 2,315,931 users around the world[1]. There are two types of ransomware, lockscreen ransomware and encryption ransomware, with the latter being viewed as one of the most dangerous types of malware ever created.

Encryption ransomware, also called crypto-ransomware, has seen a huge rise in use by hackers to extort money from victims, with a notable example being that of CryptoLocker. Targeting computers running Microsoft Windows, CryptoLocker hit the internet in September 2013 and was reported to have successfully extorted around £240,000 from victims.

[1] *http://www.kaspersky.com/about/news/virus/2016/Crypto-ransomware-Attacks-Rise-Five-fold-to-Hit-718-Thousand-Users-in-One-Year*

How does it work?

Ransomware usually spreads via a Trojan (see T), which infects a system through a downloaded file or network vulnerability (see V). Once inside the system, the Trojan runs the ransomware payload, which is what carries out the malicious action.

For lockscreen ransomware, a full-screen message is displayed which prevents the user from using the computer and accessing files. It will instruct the user to pay a sum of money to regain access and functionality of their computer.

Encryption ransomware, or crypto-ransomware, encrypts a user's files or high-value data and again asks for a sum of money for a decryption key.

Extortion is the goal with ransomware, with hackers normally using scareware tactics in order to force payment. Scareware programmes are designed to manipulate the user, usually deploying shock tactics so the victim complies with the ransomware. The scareware program, for example, could display a message which seems to come from the police about illegal activities on the computer. This tactic works in two ways – it forces the victim to pay and also stops the victim from telling others about the displayed message, as the content is embarrassing or damaging to their reputation.

Protection tips

Follow the simple rule – if unsure, don't click. Don't click on any emails or attachments from people you don't know, don't visit unsafe or fake websites and don't click on any bad links on social media. Make sure you back up your computer, use a reliable security solution and keep your computer software up-to-date.

S

Threat name

Social engineering

Social engineering is a technique used by hackers to physically (i.e. not online) manipulate people into performing an action or sharing data.

Description

Social engineering involves tricking people and at its most basic level, has been a popular confidence trick, or 'con', used by criminals for many years. In 2007, a man using just his charm tricked employees at an ABN Amro bank in Belgium and walked away with €21 million in diamonds. In 2013, the Associated Press Twitter account was hijacked after an employee clicked an email. The hijacked Twitter account sent the Dow Jones Industrial Average (DOW) plunging after tweeting 'Breaking: Two Explosions in the White House and Barack Obama is injured.' Both the diamond heist and the AP Twitter hijack are both examples of social engineering – gaining confidence in return for access, data or fraud.

How does it work?

There are numerous types of social engineering attacks – some play on the targeted person's vanity, others play on authority and greed. And many are incredibly simple. One method involves leaving an infected device, such as a USB stick, lying around, in the hope that someone picks it up and plugs it into their machine. The stick would then install malware or a virus. Another commonly used technique is called phishing – see P for more information.

Protection tips

It's wise for businesses to give all employees training and guidance on social engineering. When employees are trained in security protocols and told how data and information should be handled, a successful attack is much less likely. It's also a good idea to have a framework of trust and an assessment of risk in place, with employees only given access to data that's within their remit.

T

Threat name

Trojan Horse

Often disguised as legitimate software, a Trojan Horse is a type of malware that hides its malicious intent in order to hack into a computer.

Description

The Trojan term given to this form of malware stems from the well-known Ancient Greek story, which saw the Greeks trick the Trojans with a huge wooden horse. The term 'Trojan Horse' has now come to describe any hoax or trick that causes someone to invite an enemy into a secure place – and Trojan malware is no different. If a Trojan is successfully installed, the malware then normally has full access to the system. With this unlimited access, the hacker can do a number of things: crash the computer, recruit the machine as part of a botnet (a network of private computers infected with malicious software and controlled as a group), steal data, install ransomware or spy on the user.

How does it work?

Usually, a social engineering (see S) technique is used to trick users into loading and executing Trojans on their computer. For example, a user may unintentionally download a Trojan via a drive-by download, or may be tricked into opening an attachment on an unassuming email. The payload, or action, of the Trojan depends on what it's been designed to do – a backdoor Trojan (see 'B') gives hackers remote control over the infected computer, while a Trojan-Banker steals account data for online banking and e-payment systems.

Protection tips

The first step in protecting against Trojans is to install a reliable, effective anti-malware product. A good anti-malware product should detect and prevent Trojan attacks on your computer and devices. It's also advisable to use an Internet service provider that has strong anti-spam and anti-phishing procedures.

As Trojans are spread through social engineering, it's important to avoid anything that seems malicious, out-of-place or that comes from an untrustworthy source. Remember – if unsure, don't click.

U

Threat name

Unauthorised access

Illegal access to a website, program, server, service or data. It's more popularly referred to as hacking.

Description

Unauthorised access is the use of a computer or network without permission and is illegal in many countries worldwide.

How does it work?

Unauthorised access is usually distinguished by internal or external attacks and can be accessed in a number of ways. Weak, stolen or lost credentials are among the most common methods used to compromise a computer and bypass access control. A hacker could also infect the target with malware using, for example, a Trojan, or exploit a vulnerability in the operating system, hardware or applications. Hackers could also use social engineering (see S) tactics, as well as using tools like a keylogger to gain unauthorised access to a computer or network. With an internal attack, access could be gained through theft of other users' credentials, or someone with high-level privileges could be bribed to access information for a malicious third-party. In fact, research from BT and KPMG has found that 51% of companies don't have a strategy to deal with blackmail.

Protection tips

Weak and lost credentials are an easy win for those trying to gain unauthorised access to a system, so a clear password policy is a must in any business. To protect against vulnerabilities and bugs, make sure that you apply the latest security patches – these might plug the security holes a hacker uses to gain unauthorised access. It's also a good idea to review network security privileges – only give employees access to data and areas which are within their remit, as both non-IT and IT personnel rarely need all the keys to the kingdom.

V

Threat name

Vulnerabilities

In this context, the term ‘vulnerabilities’ refers to bugs in software programs that leave computers open to hacking.

Description

One of the most famous vulnerabilities of recent times is the Heartbleed bug. This is a serious vulnerability in the popular OpenSSL software, which is used to secure communications between computers. When the vulnerability was disclosed in April 2014, around half a million of the Internet’s secure web servers were believed to be vulnerable.

How does it work?

Vulnerabilities can be design flaws or programming mistakes included in the code of a piece of software. They can be exploited in a number of ways. Heartbleed was particularly dangerous as it exposed both passwords and login credentials, as well as the secret keys used to keep this sensitive information secure.

Protection tips

To protect yourself against vulnerabilities, it is a good idea to update your software whenever new versions are available, and download any patches that may be released for it. If any software is present that is no longer supported by the vendor, restrictive firewall rules should be turned on to stop the host from accessing the internet, and other hosts from accessing the vulnerable service.

W

Threat name

Web vandalism

Web vandalism is where a hacker gains access to someone's website without them knowing, and defaces it.

Description

Web vandalism can be seen as a kind of 'electronic graffiti', and can be used by 'hacktivists' to spread politically motivated messages or, in some instances, to cover up other malicious behaviour being carried out by the hacker elsewhere on the server.

In 2012, Google's Pakistan page, Google.com.pk, was vandalised along with hundreds of other .pk domains (domains hosted in Pakistan). On the Google page, the logo was removed and replaced with a picture of two penguins.

How does it work?

A hacker will get access to a web server through abuse of a vulnerability or through weak credentials, after which they're free to change the content of the website to whatever they want.

Protection tips

To protect yourself against web vandalism, you should make sure that:

- your operating system and software is up-to-date
- any file systems used to store static content in web servers are configured as read-only
- databases that hold web content are secure, in separate demilitarised zones (internal network systems with limited access to those outside of an organisation)

You could also implement stronger authentication (such as two-factor authorisation, where security such as a text pass code is used alongside a password for entry) for administrators to make changes. Finally, file integrity monitoring an internal control or process that validates the integrity of operatingsystem and application software files, can alert administrators when anything changes.

X

Threat name

XSS

Cross-site scripting, nicknamed XSS, refers to a type of computer security vulnerability that is usually found in web applications.

Description

XSS is a code injection attack, where an attacker can execute malicious scripts within a website or web application. By embedding the malicious script, or a 'payload', within the input that's submitted to web pages, an attacker can make the victim's browser run the malicious code. There are two common variants of XSS: stored or reflected. A stored XSS attack means the payload (the part of the malware that performs the malicious activity) is stored on the website permanently. A reflected XSS attack means that the payload is more of a one-off, where the user has to load a link that the attacker sends to them.

How does it work?

If anything a user inputs to a web server can be returned on a different page, such as leaving a comment on a video, the website could be vulnerable to an XXS attack. If an attacker inputs data that can be represented as part of the website's code, the site is again vulnerable to an XSS attack. To prevent this, information that is sent to or from a web server should be sanitised so it doesn't contain anything that could be interpreted as code.

Protection tips

Both reflected and stored XSS can be addressed by performing the appropriate validation and escaping on the server-side. When developing web applications, it's a good rule of thumb to assume that all data received by the application is from an untrusted source. So you should validate it for type, length, format and the range for whenever data passes from a web form to an application script, and then encode it before redisplaying in a dynamic page. Before a website or application goes live, it should be penetration tested in order to flag up any XSS flaws.

Y

Threat name

YTCracker

Bryce Case Jnr., aka 'YTCracker' is a former hacker turned hip hop artist, who is best known for defacing several US government websites.

Description

Starting in 1999, when he was a seventeen-year-old high school student, YTCracker defaced a number of websites, including NASA's Goddard Space Flight Centre, the Bureau of Land Management's national training centre, the Defense Contract Audit Agency, Airspace USA, Altamira, Nissan Motors, Honda, the monitoring station for the United States Geological Survey, and the Texas Department of Public Safety.

Despite claiming that he broke into the websites in order to alert them of security problems rather than with malicious intent, in May 2000 he was charged with criminal mischief and computer crime for breaking into the Colorado Springs city website, causing an estimated $25,000 in damages.

How does it work?

When defacing the website of NASA's Goddard Space Flight Center, YTCracker used a modified front-end for a common msadc.pl exploit. The exploit takes advantage of a security flaw, such as software vulnerability via an attack script. In this instance, the hacker did this to take over the front page of the website. The page placed there showed a cartoon of a hooded figure with a peace symbol, along with a message warning of the dangers of website security flaws and cyberattacks.

Protection tips

To protect against hackers such as YTCracker, make sure that your networks and systems are regularly penetration tested – a penetration test is a pre-arranged attack on a computer system that looks for security weaknesses. And keep up-to-date with any necessary software patches and version updates that may have been released.

Z

Threat name

Zombie

A zombie is an Internet-connected computer that has been compromised by a hacker or virus, and can be controlled remotely in order to carry out malicious activities.

Description

There's a big market in taking ownership of other people's computers without their consent. Hackers infect thousands of machines so they can be remotely controlled. This forms a network of 'zombies' called a 'botnet'.

How does it work?

Owners tend to be unaware that their machines have become zombies. Infection is usually automated, so most members of the botnet are likely to have run a programme they shouldn't have or left their machine unpatched.

Once infected, zombies can be used for anything the hacker wants. They can be used to bring down websites by bombarding them with traffic until their webservers crash, to send spam, or to infect more machines. Once the hacker is finished, they can simply sell the botnet to someone else.

Protection tips

To protect a computer against becoming a zombie, install/update your anti-virus software and make sure you have a firewall in place. You could try tracking all incoming and outgoing traffic to identify repeated requests from the same application targeting a few destinations – this can often be a sign of a zombie application. It's also a good idea to delete spam email messages without opening them, and never open their attachments. Avoid downloading applications that don't come from a trusted source. If you believe your computer has been infected and you want to be sure you have removed all traces of its zombie past, it makes sense to back up your files, then wipe your hard drive and reinstall your operating system from scratch.

HISCOX

A comprehensive guide to cyber security for small businesses.

https://www.hiscox.co.uk/business-blog/