An Introduction to Cybercrime

Martin Hynes

Business Computer Solutions

Cyber-crime is any illegal activity that involves computers and a network. The computer may have been used in the commission of a crime, or it may be the target.

A National Audit Office report published in 2013 suggested that the cost of cyber-crime to the United Kingdom costs around £27 billion every year. Hackers are getting more sophisticated in how they access your sensitive information. Their goal is to gain unauthorised access to your data using methods such as phishing and cyber-attacks.

Here are some methods that hackers use:

Fake wireless access points – Anyone using a piece of software and a wireless network card can advertise their computer as an available wireless access point, which is then connected to the real, legitimate wireless access point (WAP) in a public location.

Always protect confidential information sent over a wireless network. Consider using a VPN connection which protects all your communications.

Cookie theft – When a hacker steals your cookies, they assume your identity which is an increasingly frequent occurrence. They become authenticated to your websites as if they are you, as if you had supplied a valid log-on name and password.

Even encrypted cookies can be stolen. Only connect to websites that are secure.

Bait & switch – At first you are downloading or running one thing, which will last for a short amount of time, but then it is switched out with a malicious item.

Beware of any link to any content not under your direct control because it can be switched out on a moment's notice without your consent.

According to this report, 8% of UK businesses have experienced at least one type of cyber-crime. On a more positive note, those who had suffered some form of cyber-crime said the experience had shocked them into becoming more secure, with almost half (45%) opting for stronger passwords and 42% saying they were now more vigilant.

Is Your Business Safe From Cyber-Attacks?

UK businesses are battling a huge rise in cyber-crime, capable of shutting down entire companies for hours, days and even weeks. According to a report published this year by PwC Global, here are some UK based statistics:

• 55% of UK organisations have fallen victim to cyber-crime in the past two years.
• More than one in three organisations report being victimised by cyber-crime.
• Cyber-crime is ranked as the second most reported financial crime, affecting 32% of organisations.
• 61% of Managing Directors are concerned about their security, yet only 37% of organisations have a plan in place, in the event their organisation is targeted.

Today, all industries are at risk – including some which may have considered themselves unlikely targets in the past. According to PwC's Global State of Information Security Survey 2016, the sector registering the most significant increase in cybercrime activity in 2015 was retail.

Do businesses need more education and understanding of the threats of cyber-crime and how to prepare for them? "Businesses are a major target for fraudsters and these figures illustrate the significant rise in Action Fraud reports," said the City of London Police's Commander Chris Greany and Police National Coordinator for Economic Crime. "The true figure will be much higher and businesses need to take steps as many of these crimes could be prevented."

As cyber-criminals become increasingly more sophisticated, strategic and bolder in their attacks, cyber-crime continues to become a growing threat and serious concern for organisations, all over the world.

What is Social Engineering?

When you hear the term '***social engineering***,' do you want to run in the other direction and pretend you didn't hear? Fear not; we are here to help because the reality is, if you don't know what *social engineering* is, you need to.

Social engineering is the art of manipulating people, so they give up confidential information. As human beings, we trust people and what they say. *Unfortunately, we live in a world where people will take advantage of this.*

Criminals use social engineering tactics because it is usually easier to exploit your instinct to trust, than it is to discover ways to hack your software. For example, it is much easier to trick someone into giving their password willingly, than it is for hackers to try and access their account.

When individuals are targeted, criminals are usually trying to:

- Trick you into giving them your passwords or bank account information.
- Access your computer to secretly install malicious software that will give them access to your passwords and bank information, as well as giving them control over your computer.

What is Social Engineering?

The weakest link in security is inevitably the person who accepts a person or scenario, at face value. It doesn't matter how many locks are on your doors, how many guard dogs are barking, alarm systems and armed security are available; if you trust the person at the door who is delivering a big bunch of flowers and you don't' ask for identification, you are completely at risk. ***Fact.***

So, the question is, how do you spot common social engineering attacks?

You have received an email which contains a link: Be wary of any email you receive! If the link comes from a friend and you're curious, you'll trust the link and click on it. Hackers have become so clever that they can make an email look like it is has come from a friend, when in fact it hasn't. Once you have clicked on the link, your computer can be infected with malware and the criminal can take over your machine.

Best advice; check the language used in the email. Is it the usual language used by your friend? Also, when you can hit reply, you can check the email address. **Check both before you click on any link.**

You have received an email which contains a download : Again, be wary! Pictures, music, films, documents and eBooks that has malicious software embedded look legitimate. *That's the problem.* If you download these, thinking it is from your friend, it's too late. Now, the criminal has access to your machine, email account, social network accounts and contacts and the attack spreads to everyone you know.

Best advice; check the language used in the email. Is it the usual language used by your friend? Also, when you can hit reply, you can check the email address. **Check both before you click on any link.**

Email from a friend: If a criminal manages to hack into or *socially engineer* someone's email password, they will have access to that person's contact list. Most people use one password for all platforms, so the chances are they will probably have access to that person's social networking contacts as well.

What is Social Engineering?

Once the criminal has that email account under their control, they can send emails to all the person's contacts or leave messages on all their friend's social pages. ***These messages may use your trust and curiosity and create a compelling story.***

Best advice; check the language used in the email. Is it the usual language used by your friend? Pick up on the phone and call them; double check!

Social networking safety is often overlooked. This can leave you vulnerable to being a target for cyber-criminals and possible reputational damage.

Identity theft is any kind of deception, scam, or crime that results in the loss of personal data, including the loss of user names, passwords, banking information and credit card details. Your phone or tablet that you are carrying around is essentially a small computer, which could suffer from malware, spyware and viruses in exactly the same way.

What is Social Engineering?

You can follow these simple steps to ensure your sensitive information and privacy are protected:

- **How much is too much?** It goes without saying, it is obviously a terrible idea to post your personal phone number, credit card information or home address anywhere on the internet. You never know who will be able to see that information, even if you are sharing it with a closed network of friends. *Only share information you are happy for people to see.*
- **Beware of people attempting to connect with you**: Anyone can pretend to be whoever they want on the internet. Online scammers present themselves as honest people with an intention to gain access to your personal information for their own purposes. When in doubt, ignore the request or better still, block the user in question.
- **Optimise your privacy settings:** Social media networks are not designed with your privacy in mind and you will always have to make manual adjustments. Go into your privacy settings, and see where things are set. Never leave any personal information set to be viewed by the public, unless you are happy to do so. If you're a stickler for privacy, there are many things you can set to only be visible by you, including your posts.
- **Always trust your gut! Ultimately, you should trust your gut**. If you post close to none of your personal information on the internet, you are significantly reducing the risk to your personal security. Remember that you don't have to make something public if you only want to share it to a small group of individuals.

When you hear the term 'Trojan Horse', do you think back to Greece and that epic horse that is one of history's most famous tricks?

Trojan Malware takes its name from the classical story of the *Trojan Horse*, because it imitates the technique to infect computers. *A Trojan* will hide within a seemingly harmless program, or will try to trick you into installing it.

What Is a Trojan Horse?

Trojans do not replicate by infecting other files or computers. Instead, they survive by going unnoticed. They may sit quietly in your computer, collecting information or setting up holes in your security, or they may just take over your computer and lock you out.

Due to Trojans being so versatile and with their ability to go unnoticed, their popularity has exploded and unfortunately for us, they have become the malware of choice for many online criminals.

Some of the more common actions that Trojans take are:

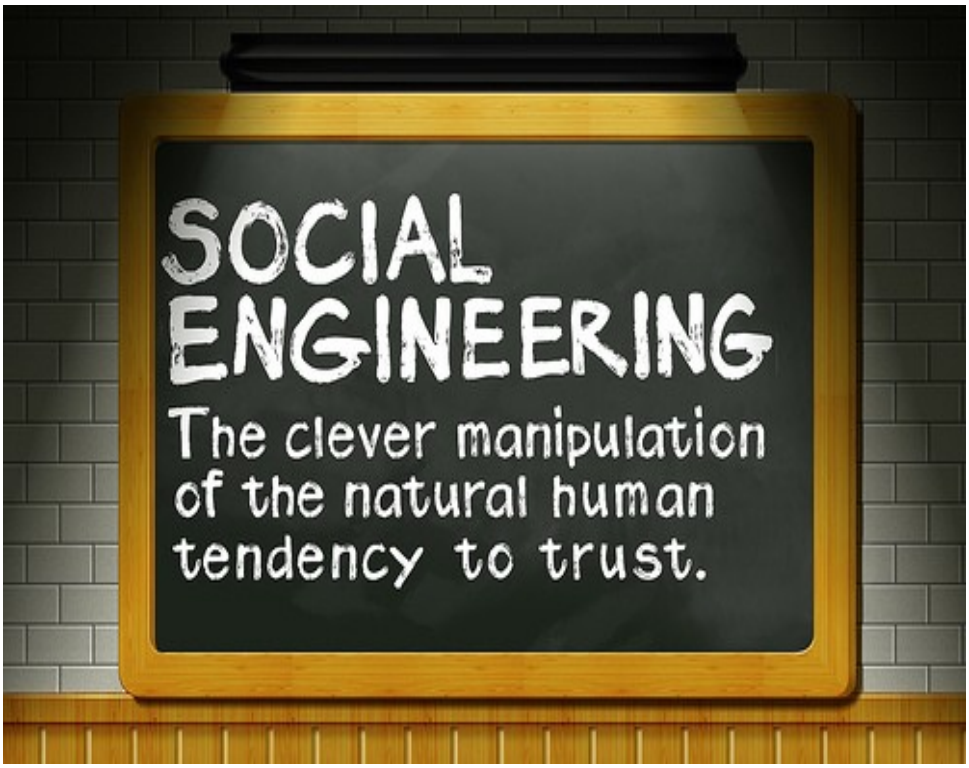
- **Creating 'backdoors':** *Trojans* typically makes changes to your security system, so that more malware or even a hacker can get in.
- **Spying:** Some *Trojans* are essentially *Spyware*; designed to wait until you access your online accounts or enter your credit card details. Then, they send your passwords and other data on for criminals to use.
- **Turning your computer into a zombie!** Sometimes, a hacker isn't interested in you, but just wants to use your computer, in a network under his or her control.
- **Send costly SMS messages:** Even smartphones get *Trojans*. The most common way for criminals to make money, is by using them to make your phone send costly SMS messages to premium numbers.

What Is a Trojan Horse?

What does a Trojan Horse look like?

Well, that's just it: Trojans can look like just about anything. The computer game you downloaded, a free song that you downloaded and even an advertisement might try to install something on your computer.

Some *Trojans* are specifically designed to trick you into using them. They can use misleading language or try to convince you they are a legitimate application. Tricking you this way is called *social engineering*, because the criminals designed a situation to make you act against your interest.



What Is a Trojan Horse?

How do I protect myself against Trojans?

1. Realise that you are an attractive target to hackers. Don't ever say *"It won't happen to me."*
2. Practice good password management. Use a strong mix of characters and don't use the same password for multiple sites. Don't share your password with others, don't write it down and don't write it on a post-it note attached to your monitor, *ever!*
3. Never leave your devices unattended. If you need to leave your computer, phone or tablet for any length of time, no matter how short, lock it up so no one can use it while you're gone. If you keep sensitive information on a flash drive or external hard drive, make sure to lock it up as well.
4. Always be careful when clicking on attachments or links in email. If it's unexpected or suspicious for any reason, don't click on it. Double check the URL of the website the link takes you to. ***Think you can spot a phoney website? Try this Phishing Quiz.***
5. Sensitive browsing, such as internet banking, should only be done on a device that belongs to you and on a network, that you trust. Whether it's a friend's phone, a public computer or a cafe's free Wi-Fi—your data could be copied or stolen.
6. Back up your data regularly and make sure your anti-virus software is always up to date.
7. Be conscientious of what you plug in to your computer. Malware can be spread through infected flash drives, external hard drives, and even smartphones.
8. Watch what you're sharing on social networks. Criminals can befriend you and easily gain access to a shocking amount of information; where you went to school, where you work, when you are on holiday—that could help them gain access to more valuable data.
9. Be wary of social engineering, where someone attempts to gain information from you through manipulation. If someone calls or emails you asking for sensitive information, it's okay to say no. You can always call the company directly to verify credentials before giving out any information. Never openly give information out if you don't feel comfortable with who you are speaking to.
10. Be sure to monitor your accounts for any suspicious activity. If you see something unfamiliar, contact your in-house IT department or Managed Service Provider straight away. That's what they are there for!

What is Malware?

When you hear the term 'malware,' do you want to hide under your desk and cover your ears? Do you feel completely lost hearing this terminology? *Fear not, you are not alone!*

Malware is short for *malicious software*, which refers to a type of computer program designed to infect someone's computer and inflict harm on it, in multiple ways. Malware can infect computers and devices in several ways. It comes in several forms; just a few of which include viruses, worms, Trojans, spyware and more. It's vital you know how to recognise and protect yourself from malware.

What is Malware?

Here are the different forms of malware with their meanings, so you can learn more about them:

- Malware – A buzz word for intrusive software, including computer viruses, Trojan horses and adware.
- Adware – Software that automatically downloads or displays advertising banners or pop ups when you are online.
- Spyware – Software that enables you to obtain information about another computer's activities by transmitting data using their hard drive.
- Viruses – Small programs or scripts that can negatively affect the health of your computer. These malicious programs can create files, move files, erase files, consume your computer's memory and cause your computer not to function correctly.
- Worms – A type of virus that replicates itself, but does not alter any files on your machine. However, worms can still create chaos by multiplying so many times that they take up all your computer's available memory or hard disk space. If a worm consumes your memory, your computer will run very slowly and possibly even crash.
- Trojan Horses –Software programs that look like regular programs, such as games and even antivirus programs. Once they are run, these programs can do malicious things to your computer.

The next question is, *"who is creating it, and why?"* Malware today is largely designed by and for professional criminals. These criminals may employ a variety of sophisticated tactics. In some cases, cyber-criminals freeze computer data; making your information inaccessible and then demand a ransom from the users, to get that data back.

One of the many risks that cyber-criminals pose to heavy computer users is stealing online banking information, such as banking and credit card accounts / passwords. The criminal hackers who steal this information, may then use it to empty your account or run up fraudulent credit card bills in your name. They may even sell your account information on, where this confidential information fetches a good price.

What is Malware?

How do I protect myself against Malware?

- Realise that you are an attractive target to hackers. Don't ever say *"It won't happen to me."*
- Have up to date antivirus software installed on your systems. Without this, you could be in trouble.
- Install security patches. Patching helps to protect your devices and has become extremely important as part of the updating process.
- Be careful with any software you install. Contact your IT provider if you are unsure.
- Delete any unknown emails. Never download or open attachments unless you are sure it's from someone you know. If you receive emails from random people, do not open them.
- Avoid clicking on ads. Especially ads where something is bright and colourful, with the possibility that you can win a prize! Ads have become more sophisticated and interactive so that you'll be tempted to play it like a game.

Action Fraud is the UK's national reporting centre for fraud and cyber-crime, where you should report fraud if you have been scammed, defrauded or experienced cyber-crime. You can visit their website here.