Leaving the back door open...

The business IT guide to spotting and preventing cyber attacks.
Contents

Introduction 3
What do you need to know about these new threats? 4
What do these attacks look like? 7
So what can you do? 13
About K3 Starcom 15
Introduction

When it comes to business cybersecurity, we often rely on the technologies and software to do the work for us, catching every problem that arises and every mistake that we make. But threats don’t disappear just like that. Cybercriminals are successfully obtaining access to our vital business data and documents by duping staff into downloading files, clicking links and opening attachments.

Most of us are familiar with antivirus software, and with the built-in security protections that come with our computers. However, there are more threats out there than these security measures can protect you against, and these threats are changing all the time, making it more difficult for antivirus and ransomware software to detect and purge your system of these attacks.

What makes these attacks so clever is the ability to appear like a normal attachment, file or link. Herein lies the problem with relying on antivirus software; it simply cannot catch every incoming attack. But you can!

You can have the most robust protection available to buy, but they might all be worthless if you let the attack in, known as ‘leaving the back door open’. This is one weakness that technology alone will not be able to stop, so knowing what these attacks are and how to recognise them will be vital in ensuring that everyone can maintain a frontline defence.

This guide aims to help you educate staff and colleagues on the different types of attack that cybercriminals are using, what they look like and how you and your team can be a strong first line of defence.

It doesn’t have to be a hard sell, either. Making internet security everyone’s business is the best way to ensure that you keep a consistent line of defence against malicious attacks, both known and unknown. A layered approach to defence can help companies be more prepared for attacks and reduce the number of successful attacks taking place.

So let’s stop these cybercriminals in their tracks and slam the back door in their faces… Once and for all.

“At K3 Starcom, we have seen first-hand the damage that a poor judgement call can wreak on a business’s security and technology. Educating your staff is a crucial part of maintaining a frontline defence against cyberattacks, but it is short-sighted to assume everyone has the same level of IT literacy or exposure to attempted attacks. This is simply not the case.

“Arming your employees with the latest up-to-date advice and tips will keep more attacks at bay, creating a safer working environment for everyone. We hope that this guide educates and informs your workforce, so share it far and wide.”

Stuart Buckley, Sales Director, K3 Starcom
What are these modern threats?

Encrypted attacks are on the rise

According to the 2017 SonicWall Annual Threat Report, approximately 60% of modern Internet traffic is encrypted. This sounds good, but actually it means that a large proportion of your company’s incoming traffic could bypass regular protection software. Malware distributors know this is a soft spot in many networks, and are increasingly keen to exploit it.

You can send an encrypted email, and only the recipients with a key can read it. Use an encrypted internet connection and you’ll find that your information – including things like banking details – are hidden from unauthorised users like hackers and identity thieves.

But these methods are the precise ones that hackers are using to deliver their attacks. Services like Transport Layer Security (TLS), Secure Sockets Layer (SSL) and Secure Shell (SSH) protocols can all be manipulated by the hacker to exploit vulnerabilities, push malware downloads, conduct command and control communications and steal data from inside encrypted traffic.

What is encryption?

Encryption protects the assets that we keep on our computers, databases, servers and devices by using computers and algorithms to turn plain text into incomprehensible code, which can be decrypted with an encryption key.

<table>
<thead>
<tr>
<th>Passphrase</th>
<th>this is the default phrase</th>
</tr>
</thead>
<tbody>
<tr>
<td>Encrypt with phrase</td>
<td>Decrypt with phase</td>
</tr>
</tbody>
</table>

Text to encrypt or decrypt

--- Start of mailencrypt ---

ZZZZZ BXNTF JQREB SGORB LEFTGY JAETF CCHYRB ZZSWJF ISTTRI KAIASO KAAEIRC HAWQKOJ AIJEF CDDAE BXNTF JQREB SGORL LEFTGY JAETF CCHYRB ZZSWJF ISTTRI KAIASO KAIERNC HAWQKOJ AIJEF CDHML BXNTF JQREB SGORL LEFTGY JAETF CCHYRB ZZSWJF ISTTRI KAIASO KAAEIRC HAWQKOJ AIJEF CDDAE BXNTF JQREB SGORL LEFTGY JAETF CCHYRB ZZSWJF ISTTRI KAIASO KAIERNC HAWQKOJ AIJEF CDHML BXNTF JQREB SGORL LEFTGY JAETF CCHYRB ZZSWJF ISTTRI KAIASO KAAEIRC HAWQKOJ AIJEF CDDAE BXNTF JQREB SGORL LEFTGY JAETF CCHYRB ZZSWJF ISTTRI KAIASO KAAEIRC HAWQKOJ AIJEF CDDAE BXNTF JQREB SGORL LEFTGY JAETF CCHYRB ZZSWJF ISTTRI KAIASO KAAEIRC HAWQKOJ AIJEF CDDAE BXNTF JQREB SGORL LEFTGY JAETF CCHYRB ZZSWJF ISTTRI KAIASO KAIERNC HAWQKOJ AIJEF CDHML BXNTF JQREB SGORL LEFTGY JAETF CCHYRB ZZSWJF ISTTRI KAIASO KAIERNC HAWQKOJ AIJEF CDHML BXNTF JQREB SGORL LEFTGY JAETF CCHYRB ZZSWJF ISTTRI KAIASO KAAEIRC HAWQKOJ AIJEF CDDAE BXNTF JQREB SGORL LEFTGY JAETF CCHYRB ZZSWJF ISTTRI KAIASO KAIERNC HAWQKOJ AIJEF CDHML BXNTF JQREB SGORL LEFTGY JAETF CCHYRB ZZSWJF ISTTRI KAIASO

--- End of mailencrypt ---
Ransomware

In 2015, ransomware accounted for a miniscule 2% of emails with malicious links or attachments, but in 2016, accounted for 97%. Its phenomenal growth as a tool for destruction has gone mainstream. WannaCry, Petya and Locky are just some of the successful attacks that have cost businesses, organisations and governments across the world significant headaches over recent years.

Once running on a user’s PC, the software then locks them out of their computer, sometimes pretending to be a law enforcement agency. Typical claims are that the machine has been used to look at pornography or ‘pirated’ media – obviously things you would not want to be accessing at work!

The hacker, having successfully added an emotional punch to proceedings, can then demand as much money as they like. Ransomware can travel across the network a compromised computer sits in, as was seen with the WannaCry worm – but this is not always the case.

Ransomware attacks are now carried out on an industrial scale, with smarter attacks catching more people out.

What is Ransomware?

In short, ransomware is malicious software that blocks access to a computer or system until a sum of money is paid, usually in cryptocurrency like Bitcoin. Hackers entice users to download and open the malware when it arrives as an email attachment (a process known as social engineering, but more on that later) or from visiting a compromised website that downloads the file to your PC (and we’ll explore this later on too).
Social engineering

Time to talk about social engineering; the tactics that hackers will employ to convince you of their apparent legitimacy.

Social engineering is growing in popularity by attackers because, as you can see, they prey on the most vulnerable asset that any business will have – its people. Criminals use these tactics because it’s easier to exploit our natural inclination to trust what we see than it is to corrupt software.

They also use visual identifiers that we will recognise, such as the company’s logo and tone. These emails will look like they’re from a large retailer or tech company and they often use use large, well known brands to appear more realistic.

What is social engineering?

These attacks rely heavily on human psychology, our natural curiosity and our innate desire to help or to be nosey. One of the many examples we have seen over the years is when the attacker pretends to be a colleague, emailing to ask the recipient for help, and they then click on the attachments or a URL that infiltrates the user’s PC and wider network.

To find out more about the security services that K3 Starcom offers, visit our website.

starcom.tech/managedsecurity
What do these attacks look like?

It's not just enough for you to know what is out there and pass this information onto your staff; each attack has its nuances and we know that more threats are being created, so it is crucial for you to understand what these attacks look like, how they impact your IT network and where you might find them… This is advice for everyone in the office, so please feel free to share it around!

Social Engineering

Phishing

Hackers send fraudulent emails from a trusted source to any email addresses they can find. They claim to need personal information and that you can supply this via a link or by downloading the attached form – except there is no form.

Spear phishing/whaling

It's a small scale, highly-focussed phishing attack. Criminals design each individual attack and techniques to effectively personalise messages and websites. This may appear to be a real email, even to C suite executives. These emails may mimic the company’s email format, be from a source they trust – the CEO, HR department or accounts, for example – and contain luring subjects or attachments, like a file called ‘Annual Group Expenses’. Tools like this incite the reader to access something they think is for their eyes only.

Baiting

Preying on our instinctive curiosity, hackers drop malware-infected USBs in communal areas or outside buildings and hope that staff blindly insert these USBs into their computer, allowing the malware to spread across an entire network very quickly.

Email from a friend

Once a hacker has access to one user’s data, they can then start to trawl their address books to continue spreading viruses and malware. People trust their friends, so are more inclined to click on links that you ‘need to check out!’ or contain a malicious download.

Pretexting

A usual pretext attack takes the form of the attacker pretending that they need this information to confirm the recipient's identity and lure the recipient into a sense of trust, by claiming to be a colleague or from government agencies such as HMRC and Companies House, for example.
Don’t take the bait!

This example highlights where the hacker is using our innate sense of trust – it’s an email purporting to be from this company’s CEO and has the innocuous attachment, Annual Group Expenses. Now, staff would leap at the opportunity to see what the Group CEO has been claiming on expenses, wouldn’t they?

If you look closely, there are several ways to spot a potentially fraudulent email. They may not all be present, but look out for poor grammar and spelling, an email address that doesn’t match the domain of the organisation, unexpected attachments – especially zipped attachments.

Do not open emails from untrusted sources! Contact a colleague or your IT department if you receive something you’re unsure of.

When receiving emails from organisations such as a bank, building society or the Government, you can reduce the risk of using a contaminated link by manually entering their URL and accessing the site that way.

What can you do?
Ransomware

Unlike other attacks that spread like a trickle, ransomware has no incubation period or warning signs. You only know your files have been encrypted once it has happened. It has crippled organisations and businesses – in fact, the 2017 WannaCry attack affected 200,000 users in 150 countries.

If you look closely, there are several ways to spot a potentially fraudulent email. They may not all be present, but look out for poor grammar and spelling, an email address that doesn’t match the domain of the organisation, unexpected attachments – especially zipped attachments.

Do not open emails from untrusted sources! Contact a colleague or your IT department if you receive something you’re unsure of.

When receiving emails from organisations such as a bank, building society or the Government, you can reduce the risk of using a contaminated link by manually entering their URL and accessing the site that way.

What can you do?
Viruses

We are more likely to be familiar with viruses and how they appear, but it does mean that we may not have kept up with how they have changed in recent years. Viruses are typically spread by email attachments and downloading illegal software and infected files from the Internet. Unless antivirus software is up-to-date and captures the virus, you often have no evidence of its appearance until something goes wrong.

Spyware

This software aims to monitor a victim’s computer usage and gather information about them without their knowledge. They are often difficult to detect and also change computer settings, make unauthorized changes to your computer’s settings and download other programmes.

Malware

An umbrella term for a number of different hurtful and intrusive software. Malware is designed to take over control of victims’ computers and carry out any number of tasks. For example, sending email spam, hosting contraband data such as extreme pornography and engaging in attacks against others.

Trojans

A particular type of malware that is often disguised as legitimate software; antivirus software, games and plug ins are often used. One installed on a user’s PC, they typically appear to be doing the job, but are in fact installing any type of malware that the cybercriminal has used.

What can be done to protect against viruses?

- Allow your antivirus programme to carry out its required updates.
- Don’t click on links within emails if you don’t recognise the sender. Use a search engine to find the website they are referring to. This will often help you see whether an unsolicited email is genuine or malicious.
- Back up your data. If an incident occurs, you don’t risk losing everything.
- Enable the firewall software that both PCs and Macs have built-in.
- Consider using an ad blocker and be amazed at the thousands of ads you no longer see, thus reducing the likelihood of an ad that sounds too good to be true…
- Has something changed but you can’t put your finger on it? If you notice new applications in the start menu, your PC opens programmes that you didn’t ask it to or your browser now has more buttons and toolbars, you may have fallen prey to an attack. Run your antivirus software and speak to your IT support.
Website spoofing

Cybercriminals have become very capable at recreating websites that we are all familiar with, from our bank’s website to online retailers with whom we may have purchased things in the past. Legitimate logos, fonts, colours and expected functionality are all used to make this site look realistic.

These sites are typically part of the attack, meaning that you will receive an email that could direct you to this site and implore victims to ‘log in’ with their personal and/or financial data. Some cybercriminals also have the tools to redirect users from legitimate sites to their spoof sites too.

Once released on the web, traffic to these sites is directed by several means – ad banners on unsecure websites, in emails sent from previous victims and simply by being in search terms as not everyone uses the same levels of in-browser protection, such as content filters (software that scans for certain terms and blocks access to pages that match any agreed phrases) and antivirus programmes.

What can be done to avoid accessing spoofed sites?

- Double check the domain name – the part of the website between www. and .com or .co.uk. If it’s not what you expect to see, leave the page.
- Is the site secure? Look for the padlock in front of the website’s URL. Most browsers now check security for you, but be aware.
- You can also check if a website is secure by whether they use ‘https’ at the beginning of the URL. If doesn’t have an ‘s’, the website is not secure, and cybercriminals could be eavesdropping.
- When a company invests in customers’ security, they are likely to want to promote this fact. This is why seals exist, so look and see if the company’s page promotes their security measures.
- Look out for bad English – be wary if the language used isn’t what you would expect. While everyone makes the odd mistake, pages written in poor English should alert you to the potential damage this site could inflict.
- Trust your gut. If you think a website is suspicious to you, then scour other pages to assess whether you trust it before putting in confidential or financial information.
SEO Poisoning

Hackers often use search engine optimisation (SEO) tactics to make their spoof websites appear prominently in a user’s search results. The sites are associated with large-scale search terms; for example, in the run up to Christmas hackers might launch a site dedicated to seasonal recipes or promote a range of free templates for Halloween costumes in September and October.

By using SEO tactics, hackers add legitimacy to their website as the victim has found their site simply by searching for it. The hacker will use private blog networks and link pyramids to quickly build their fraudulent site’s ranking, meaning that victims won’t have searched far before they land on these sites.

Users are often redirected through a host of other pages and links, while in the background the page checks the user’s security protocols, making decisions on what viruses to target towards the victim.

When users land on these tainted sites, they are often met with pop ups like the below – these alerts aim to unnerve and incite panic in potential victims, leading them to download malware of some form.

The page at http://tech-tips-2018.com says:

Warning!! Your computer contains various signs of viruses and malware programs presence.
Your system requires immediate anti viruses check! Antivirus 2009 will perform a quick and free scanning of your PC for viruses and malicious programs.

How can you spot poisonous search results?

- Poisoned pages can redirect to pages full of fake virus alerts. If you see such a screen that is trying to convince you that you already have malware, don't click anywhere in the browser and promptly close it.
- Enable the security features of your browser now. Most browsers have these features as standard.
- Ensure that all your antivirus, anti-ransomware and firewall programmes are up-to-date.
- Be as specific as you can with your searches. This reduces the chance of such a site appearing so highly in your search results.

K3 Starcom supplies advanced screening and security software to hundreds of businesses across different industries, sizes and technical requirements.

To find out how we can help protect your business, call us today on 0844 579 0800.
So what can you do?

There are many things you can educate your workforce on today that will stand you in good stead, regardless of the nature of an attack. As we have already established, cybersecurity is everyone’s responsibility, so some of this advice applies to IT managers, HR teams and individual users.

After all, everyone at an organisation is likely to come face-to-face with threats, and it’s important that this knowledge is shared across the board – and downwards.

As a user....

- Do not open emails from untrusted sources! Contact a colleague or your IT department if you receive something you’re unsure of.
- If it seems too good to be true on the internet, it probably is. Do not give strangers the benefit of the doubt.
- Request IT security training. These attacks change form constantly, so keep your business aware of threats and appropriate responses.
- Only access secure websites. If you’re unsure of an individual website, look for the padlock and correct website address in the URL bar.
- When receiving emails from organisations such as a bank, building society or the Government, you can reduce the risk of using a contaminated link by manually entering their URL and accessing the site that way.
- Monitor software installation. If it asks to install additional software and services, it is unlikely to be helping you out!
- Enter a minimal amount of authentic information about you, if there is no legal requirement to do so. Does the site you’re joining need to know the actual name of your first school, or will a dummy set of credentials do? The chances of your data being used fraudulently is dramatically reduced if it’s not real in the first place!
As someone responsible for business IT....

- Keep your antivirus software up-to-date. No software can circumvent our judgement calls, but it could prevent the issue from escalating.
- Promote the benefits of penetration testing within your organisation. You can’t be prepared for an attack if you don’t know how your organisation may be affected.
- Deploy patches as soon as they occur, if they’re not updated automatically across the network.
- Stick to company protocols, such as issuing PO numbers for purchases. This makes it easier to reconcile accounts and spot a fraudulent invoice.
- Establish and maintain a disaster recovery process, reviewing and testing the process regularly to assess your resilience against modern threats.
- Isolate and understand the limitations of legacy equipment, as they may not be capable of running up-to-date antivirus software.

As an organisation...

- Follow protocols, especially when it comes to online purchases, paying staff, claiming expenses and anywhere personal, business and financial data is exchanged internally.
- Don’t override your network’s security processes. If the software prevents you from doing a certain action, speak to the network administrator rather than carry on with what you’re doing.
- Develop personal security policies for online behaviour and review these regularly, bearing in mind how your workforce operates. What one company may insist on as best practice could significantly impact another’s way of working.
- Protect with passwords, and change them regularly. The same applies with user accounts for staff that leave – cut off all the organisational slack that comes with time, and keep user accounts and passwords fresh and up-to-date.
- Establish an Internet safeguarding policy and review it regularly to ensure that it’s capable of addressing modern threats. There is little value in a policy that is not fit for purpose.
- Ensure that the IT team, partner or agents have the time to conduct regular testing of your IT and listen to their assessments. They are the experts after all!
About K3 Starcom

Thank you for downloading and sharing this guide, we hope you found it useful and full of practical and relevant advice.

At K3 Starcom, we take security very seriously; so much so that we are launching our IT Security Lab to tackle business technology security head on and to empower our customers to keep their businesses and data safe online. Have a look at the site and sign up to find out more!

At K3 Starcom, our aim is for you to get the most possible value from your IT infrastructure, and security is just one element of this.

We design, procure, implement, manage and support an ever-growing range of solutions to help you get the most out of your technology, investment and resources.

Working together, we aim to find the solution that fits your business perfectly, from SMEs to international conglomerates. We hate working in jargon and industry terms, so we like to keep things simple and will never make IT more complicated than it really is.

We provide first-rate solutions that have the power to transform businesses, ultimately delivering a stronger bottom line and exceptional return on your investment.

Visit the K3 Starcom Security Lab today and sign up for news and invitations to exclusive business security emails.

starcom.tech/securitylab

@starcom_tech /starcom-technologies-limited 0844 579 0800 Wigan Investment Centre, Waterside Drive, Wigan, WN3 5BA