An Introduction to Cyber Security

CyberScotland

CYBERSCOTLAND PARTNERSHIP

Scottish Business Resilience Centre

Cyber Security.

Welcome to this short guide on cyber security! This document, published by the Scottish Business Resilience Centre, provides easily accessible cyber security guidance, helping you to understand common types of attacks and how to defend against them. This non-technical advice is aimed at individuals looking to improve their cyber security practices and can be read as one document or kept for future reference on individual topics.

What is Cyber Security?

Cyber security is the protection of computer systems and networks from information disclosure, theft or damage to their hardware, software, or electronic data, as well as disruption or misdirection of the services they provide.

Why is this Important?

Good cyber security practices are vital to protecting your organisation: The average cost of all breaches or attacks identified between July 2021 and July 2022 on a micro or small business was estimated at £3080. Modern cyber-attacks come in many forms, but mostly target people, rather than systems. As such, the best thing you can do is to improve your cyber security practices and your understanding of the threats. Remember, cyber security is everyone's responsibility. You should always look out for and report anything suspicious to the designated person in your organisation.

Types of Cyber Attack

A cyber attack refers to an action designed to target a computer or any element of a computerized information system to change, destroy, or steal data, as well as exploit or harm a network. As you know, cyber attacks come in many forms.

A few common examples of cyber-attacks are:

- Phishing Attacks
- Ransomware
- Password Attacks

Phishing Attacks

Phishing is one of the biggest threats facing organisations, with approximately 83% of data breaches beginning with a phishing attack. A phishing attack is a form of social engineering, in which an attacker attempts to manipulate the user into doing something they shouldn't. Typically the attacker sends communications that seem to come from trusted, legitimate sources but include a link that brings you to a website that then fools you into giving the attacker sensitive information, or downloading malware. In many cases, the target may not realise they have been compromised, which allows the attacker to pursue others in the same organisation without anyone suspecting malicious activity.

Attackers also leverage current affairs to make their attacks seem more believable, for example promising cheap covid tests or cost-of-living grants.

Advice

Generally, phishing emails can be spotted quickly if you know what to look for. Remember, if you are unsure about something or have clicked on a link that you think could be malicious, then you should always report it within your own organisation.

You can report suspicious emails to the NCSC using the email report@phishing.gov.uk

Some things to look out for:

- Poor grammar/spelling - Phishing attacks are often sent from countries outside of the UK, where English is not widely spoken. Real communications will use correct grammar!
- Nothing to identify you – Typically an email or text would be addressed to you, as in "To John". Attackers are unlikely to know this information, so the email may just be addressed "Dear customer" or similar. Look for the identifying information. Services may also include a portion of your postcode or phone number to show they are who they say they are.
- Suspicious email address – For example, "returns@roya1mai1.com" (Notice the digit '1' in place of the letter 'L'). This makes the address look real, at a glance. Be sure to examine it carefully.
- Suspicious link – Carefully examine any links in the message, and compare the real one online. If something doesn't match up, you should be suspicious.
- Sense of urgency – Malicious hackers will try to rush you into making impulse decisions, by making you panic with a fake security alert, or by offering something too good to be true like a discounted holiday. Always slow down and consider what you are being asked to do and why!
- Were you expecting it? - A common scam is to request payment for a parcel delivery or invoice that doesn't exist. Ask yourself, are you expecting a delivery? If not, it's probably fake!

Related Links

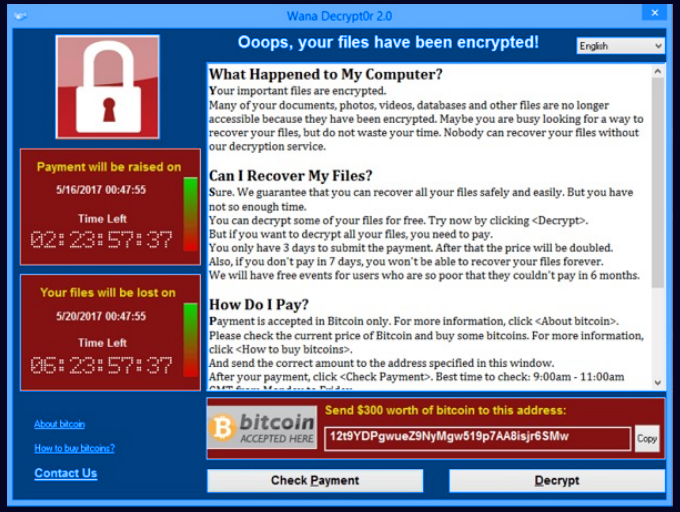
- SBRC Ethical Hacker Sarah discusses phishing and the psychology behind these attacks in her blog.
- The NCSC has also published comprehensive guidance on phishing.

Cyber Security.

Ransomware

Ransomware is a type of malware that encrypts a user's files, making them inaccessible. The criminals responsible refuse to unlock the files unless a ransom is paid, usually in cryptocurrency.

When a target is infected with ransomware, often the malware comes from within an email attachment. The malware exploits vulnerabilities that have not been addressed by either the system's manufacturer or the IT team. The ransomware then encrypts the target's workstation. Sometimes, ransomware can be used to attack multiple parties by denying access to several computers or to a central server essential to business operations.



Ooops, your files have been encrypted!

What Happened to My Computer?

Your important files are encrypted.
Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

Can I Recover My Files?

Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.
You can decrypt some of your files for free. Try now by clicking <Decrypt>.
But if you want to decrypt all your files, you need to pay.
You only have 3 days to submit the payment. After that the price will be doubled.
Also, if you don't pay in 7 days, you won't be able to recover your files forever.
We will have free events for users who are so poor that they couldn't pay in 6 months.

How Do I Pay?

Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.
Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.
And send the correct amount to the address specified in this window.
After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am

Send $300 worth of bitcoin to this address:
12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw

Figure 1 Screenshot from the 2017 Wannacry ransomware attack.

Should I pay the ransom?

No! When paying a ransom, not only are you directly funding organised crime, there is also no guarantee that your data will be given back to you or that the criminals will delete any data that they have stolen. Paying the ransom also identifies you as an attractive target, and makes it likely you will be attacked again, especially if you have not resolved the vulnerability which allowed you to be attacked in the first place.

The SBRC and NCSC have published in-depth guides on protecting yourself from ransomware.

Password Attacks

Passwords are the authentication method of choice for almost all online services, and so are an attractive target for a malicious hacker. Passwords can be targeted in many different ways, commonly through phishing attacks, but often malicious hackers will carry out credential stuffing attacks. In these attacks, hackers will use usernames and passwords taken from data breaches from other services and try them on the target service. The best defence against this is using a unique password for each service.

An attacker may also try to intercept your internet traffic to steal passwords, for example when you log in to a webpage. They can also use manipulation, such as a phishing attack, to trick the user into disclosing their credentials. In other cases, the attacker can simply guess the user's password, particularly if they use a default password or one that is easy to remember such as "1234567."

The SBRC has also published a blog on password health.

The NCSC published a blog related to passwords and how they prevent potential attackers from gaining access to your systems.

Advice

Regular password changes? Think again!

In many organisations, individuals were previously advised to change their passwords regularly as a protection against password breaches. Updated advice disagrees. Instead, the recommendation is to use a strong, unique password. This change is for 2 main reasons:

- **Constantly changing passwords has little benefit and may even be detrimental to overall security. Rather than remembering a strong, complex password, when users are forced to change their password every few months, they must learn a whole new one. In this scenario, users are far more likely to reuse passwords from other systems, choose a weaker password which is easier to remember, or slightly alter their previous password e.g., "hunter2" becomes "hunter3".**
- **With no evidence of a password breach, there is no reason to change a password. Comprehensive monitoring and logging are preferred and will indicate if a password is breached and needs to be changed.**

In the first instance, you should always follow the advice of your IT team.

Choosing a password

When choosing a password, it is important to make sure that it is unique (not used for any other service) to mitigate against "password-spraying" attacks and strong to ensure it cannot be easily guessed. The NCSC advises using the three random words technique. This technique encourages users to choose any three random words and combine them to make a unique password. For example, "coffeeboatpaper" or "birddeskprinter." This technique makes passwords more memorable while preserving their important strength and uniqueness. Add a number or symbol to the password for even better security!

Cyber Security.

Password managers

An even better solution to the password problem is password managers. These programs are used to generate, store, and autofill passwords. This removes the burden of remembering passwords from the user, allowing a unique and very strong password to be used for each service. The user needs only remember a strong password to unlock their password vault.

Password managers can also be useful for identifying phishing webpages thanks to their autofill feature. The manager will not auto-fill account credentials if the URL is not an exact match to the real page.

Your organisation may offer you an enterprise password manager, but you can also use one for your personal life!

2-Factor Authentication (2FA)

Passwords are only one line of defence. Your security can be improved further using 2-factor authentication (2FA), also known as multi-factor (MFA). This adds another layer of security, requiring users to authenticate using a one-time password (OTP), usually sent to their mobile phone, either through a text or using an app. This means that even if an attacker has access to your username and password, they will also need the code from your mobile phone to be able to log in.

Password Summary

- **Use a strong password so it cannot be easily guessed. The NCSC recommends Three random words.**
- **Use a unique password for every service to prevent credential stuffing. Password managers make this simple!**
- **Enable 2-factor authentication where possible, so even if your password is compromised, attackers will still struggle to access your account.**

What else can I do to ensure I keep my organisation safe from a cyber attack?

Attend an Exercise in a Box Session

The Exercise in a Box toolkit is an online, self-help tool from the National Cyber Security Centre (NCSC) which is designed to help organisations test and practice their response to a cyber attack. It is a free, 90-minute non-technical workshop which helps organisations find out how resilient they are to cyber attacks and practice their response in a safe environment. Scenario themes are realistic and based on the main cyber threats organisations face. It includes everything needed for setting up, planning, delivery, and post-exercise activity.

As it stands, the sessions can be run remotely or in person.

The SBRC runs the following exercises:

- **Working From Home**
- **Phishing Attack Leading to a Ransomware Infection**
- **Digital Supply Chain**
- **Micro Exercises**

If you would like to know more about Exercise in a Box, you can register here for an upcoming workshop.

Further guidance and support

CyberScotland

The CyberScotland Partnership is a collaboration between key organisations that are working together to improve cyber resilience across Scotland. You can find a variety of tools and guidance provided by these partners to help you improve your cyber resilience.

For more information and support, visit CyberScotland.com

National Cyber Security Centre (NCSC)

The NCSC is the UK's centre of expertise on cyber security.

You can find more information at www.ncsc.gov.uk

- **Read their top tips for staying secure online**
- **NCSC Top Tips for Staff**
- **Training for small organisations and charities**

Scottish Business
Resilience Centre

Oracle Campus
Blackness Road
Linlithgow
West Lothian
EH49 7LR

☎ 01786 447 441
enquiries@sbrcentre.co.uk
www.sbrcentre.co.uk
@SBRC_Scotland
in company/scottish-business-resilience-centre

A Company Limited by guarantee and registered in Scotland
No. SC170241 | VAT Registration Number: 717 2746 27

CyberScotland
CYBERSCOTLAND PARTNERSHIP