Northamptonshire Police
Cyber Investigation Team

Cyber Security

National Cyber Security Centre

East Midlands Special Operations Unit

In an emergency call **999**
For non emergencies call **101**

www.northants.police.uk

Northamptonshire Police

Fighting crime, protecting people

Common Misconceptions

- Many people do not think that they will ever be affected by cybercrime or fraud, or think that they will not be targeted by scammers
- Many people think that you need to be able to remember and identify every single fake email or scam technique to stay safe from criminals
- Many people think that Google checks all website content to ensure your search results do not contain any scams or fake sites
- Many people believe a browser padlock symbol indicates that you are on a genuine and trusted website
- Many people believe that you can hover/point to the sender's email address to ascertain who really sent the message

Secure an Online Account

- Make passwords long and strong (at least 12 characters)
- Strong passwords can be made by combining three random words

BalloonSawingBurgers	Ba!!oon^^^SawingBurgers
STRONG	VERY STRONG

- Avoid using personally relatable names, words or dates in passwords
- Never share passwords with anyone no matter who they claim to be
- Always change default passwords on new Internet connected devices
- Close dormant or unwanted accounts
- Use a different password for each account or site

Involved in a Data Breach

- One or more of your online accounts may have been involved in a data breach where your passwords or other personal details have been leaked
- Find out by using the data breach notification site: **haveibeenpwned.com** to search for any linked account data breaches using your email address

Secure an Online Account

- Enable two-factor-authentication (2FA) on all your important accounts
- This adds an extra layer of security to verify genuine account access
- Ideally use an authentication app on a trusted device



- Consider using a reputable password manager on all your devices



Protecting Your Devices

- Malware can infect computers, phones, tablets and smart/IoT devices
- Viruses, spyware, worms, Trojans and ransomware are the most common types of malware
- Spyware might secretly monitor your typing, mouse movements, web browsing and location or turn on your device's camera and microphone
- Ransomware silently encrypts your computer documents and photos before demanding payment to decrypt and recover the data
- Organisations, schools and charities are especially at risk from ransomware with cyber criminals making use of remote working

Protecting Your Devices

- Ensure default passwords have been changed on your network router, smart devices and any Internet connected cameras, toys or games
- Secure your phones and tablets using a password and/or biometric lock
- Always keep your devices, apps and other software up-to-date
- Enable Auto Updates on your computer, phone and tablet
- Use a reputable and regularly updated Anti Virus package on your PC
- Regularly backup all your important documents, photos and videos

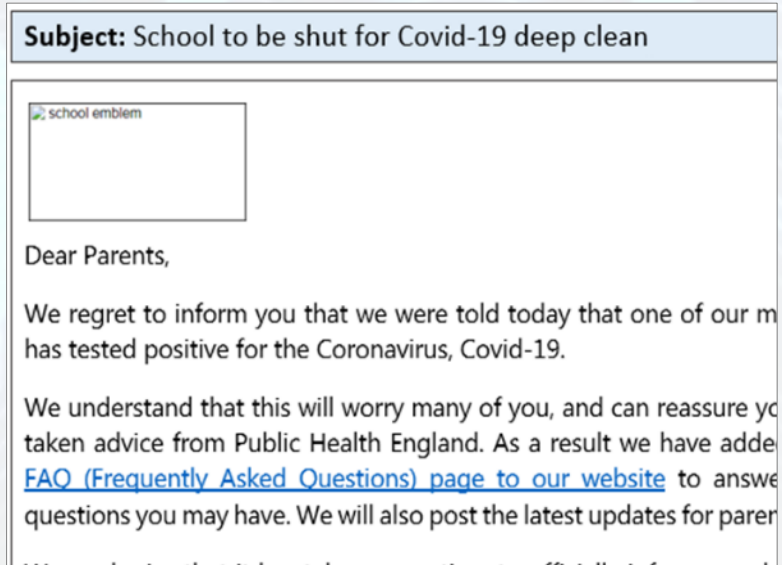
McAfee Windows Defender Norton by Symantec

SOPHOS AVG avast

Social Engineering Attacks

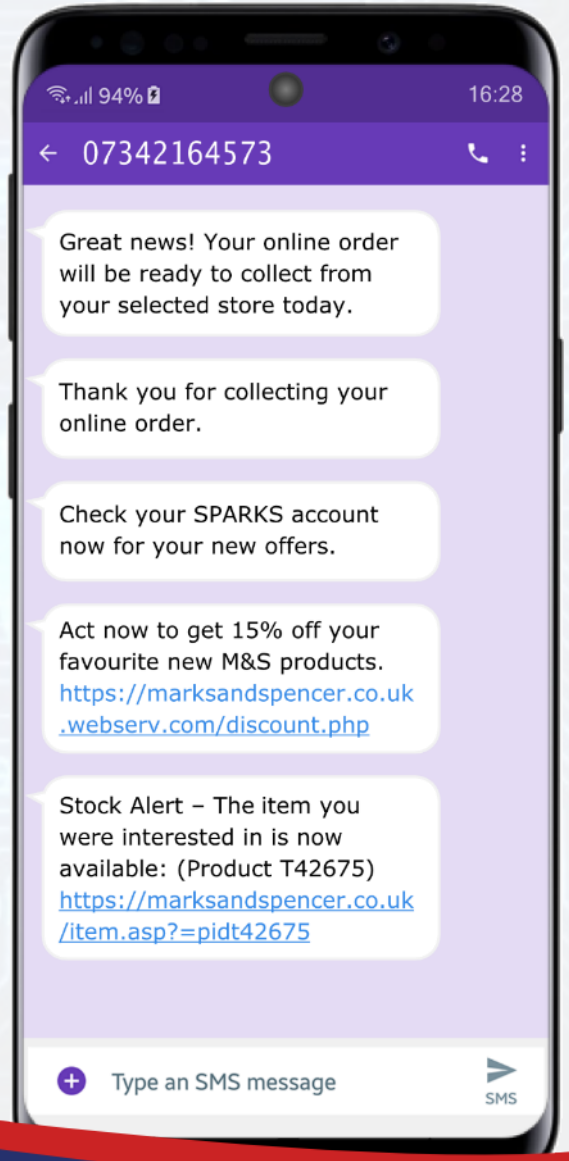
Social Engineering Attacks

- Criminals spoof the sender's address to make emails seem genuine
- Real logos, photos and other content are often used to add authenticity
- Phishing messages may appear to be from suppliers or services you use
- Emails and messages may include your name and other relevant details



Scam Text Messages

- Fraudsters send you texts, WhatsApp and other messages that may be displayed alongside your existing and trusted messages
- They may appear to have been sent by an organisation or service you know or trust
- Included links will open fake but realistic looking phishing websites or logon pages that are designed to steal your passwords, personal information and payment details
- They might also appear to be from friends or family asking for emergency funds; or for invoices, bills or fines to be paid or gifts purchased



Social engineering attacks

Never click links in unverified emails, texts and messages:

You have received a parking penalty for £60. Click here to view the photo of your vehicle and details of the incident

Your direct debit payment failed. Confirm d… void …e pa…nt cr…s.

Your HMRC tax refu… been calculated. …her… specify which …unt … war… o.

We … d m… are on your net… …ck here to protect … computer syst…

Your …it card was used to pur… BA tickets (Flight BA2… …here to can… your booking.

Your Amazon order of 'LG 55UM TV' (£589.00) will be dispatched shortly. Click here to view or cancel the order.

NEVER

CEO/Voucher Fraud

- Emailed messages appear to be from someone you know or trust
- The message may copy the content and style you are familiar with

Payment Diversion/Invoice Fraud

- Fraudsters send emails containing modified invoices and quotes, or discount offers, for genuine work or services
- They may also email you impersonating a genuine customer, supplying new payment details or a delivery location for an existing and valid order
- Spoofed email addresses, real logos and other details are often used to make them appear to be from your real customers, suppliers and staff
- Always take time to review and confirm payment changes using another trusted means of contact, such as via a verified phone number and contact already held on file

Criminals may send you emails that contain new or updated payment details and requests.
They may include valid names and details, and appear to have been sent by this company.
Always confirm payment changes by phoning the number on your initial quote.

Report these to Action Fraud via actionfraud.police.uk or 0300 123 2040 - Northamptonshire Police Cyber Protect

Computer Software Service Fraud

- Fraudsters phone you, purporting to be IT support or that they are calling on behalf of your computer, phone, software or Internet provider
- They will claim that they have identified problems with your device or Internet connection which need fixing immediately, and can be extremely convincing and manipulative
- Then instruct you to change settings, press certain keys or download remote access software such as TeamViewer
- Pop-up messages or alerts may also appear, claiming to have detected viruses or other security issues, with instructions to call a fake service line for support

Free Cyber Security and Fraud Resources

Main Points

- Make all of your passwords long and strong
- Use a different password for each account or site
- Enable two-factor-authentication on all your important accounts
- Never click links in unverified emails, texts and messages
- Verify all invoice, wage and payment change requests
- Make all staff, volunteers, members, etc. aware of the risks and advice
- Report all Cybercrime & Fraud to Action Fraud
- Contact the Cyber team for Cyber Security and Safety Resources

Report all Cybercrime and Fraud to Action Fraud 0300 123 2040

Northamptonshire Police Cyber Protect

Amie Freeman & David Reed

cyberprotect@northants.police.uk