



# Cyber Awareness

Lee Stripe & Kieran Hall


Cyber Protect & Prevent Officers

# Cybercrime...

What are they on about?



# Cyber Dependent Crime



Where a digital system is the target as well as the means of attack.

Examples include:

**Malware** – Disrupts and damages specific systems with various outcomes.

**DDoS** – Paralyse an online server by flooding it with traffic from a number of other systems.

**Hacking** – The act of gaining unauthorised access to data in a system or computer.



# Cyber Enabled Crime

Where an 'existing' crime has been transformed in scale or form by use of the internet

Vast array of crimes, most commonly:

- Fraud (Phishing)
- Extortion / Blackmail
- Harassment / Stalking
- Theft
- Sexual abuse / exploitation
- Threats to kill
- Hate crime
- Malicious Communications



DEVON & CORNWALL  
CONSTABULARY



Regional Organised Crime Unit

## SOUTH WEST POLICE ROCU

**NCA**  
National Crime Agency

National Cyber  
Security Centre  
a part of GCHQ

# WHAT IS A CYBER ATTACK?

- ❑ **Malicious attempts to:**
  - Damage
  - Disrupt
  - Or gain unauthorised access
- ❑ **...to computer systems, IT networks or devices (such as laptops, phones, tablets)**

00101110011110  
11001010100101  
11011010101101  
1011**HACKED**1111  
01010010000101  
01010101010101  
10011111101100

# WHAT IS CYBER SECURITY?

- ❑ Reducing risk of becoming a victim of a cyber attack
- ❑ Protection of devices, services, networks and the information we store on them
- ❑ The internet is a fundamental part of modern life, and so cyber security must be too



# #1 Create a separate password for your email

## Create a separate password for your email

Your personal email is the **gateway** to your other online accounts.

If your email account is hacked, not only will cyber criminals have access to important information about you, but all your other passwords can be reset.

**Use a strong password – different to all your others.**



# 2

## #2 Create a strong password using ThreeRandomWords

# Create a strong password using three random words

Weak passwords can be hacked  
in seconds.

Make your password long, strong and  
difficult to hack by using a sequence of  
three random words you'll remember.

EXAMPLE: **WaterPhilosophyZebra**

You can make it even stronger with  
special characters.

EXAMPLE: **Water!PhilosophyZebra\$**



# #3 Save your passwords in your browser

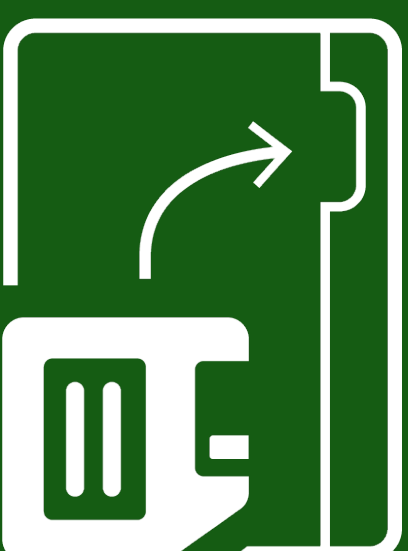
---

## Save your passwords in your browser

Using the same password for all your accounts makes you vulnerable - if that one password is stolen all your accounts can be accessed.

It's good practice to use different passwords for the accounts you care most about, but remembering lots of passwords can be difficult.

**Saving to your browser is quick, convenient and safer than re-using the same password.**



# #4 Turn on two-factor authentication (2FA) |

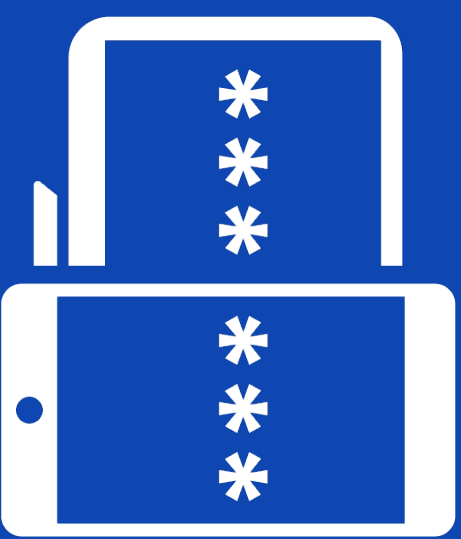
## Turn on two-factor authentication (2FA)

2FA is a free security feature that asks you to provide a second piece of information to check you are who you say you are.

EXAMPLE: getting a text or code when you log in.

This extra layer of protection stops cyber criminals getting into your accounts – even if they have your password.

If the online services and apps you use offer it, turn it on.



# #5 Update your devices |

# Update your devices

Cyber criminals exploit weaknesses in software and apps to access your personal data. Providers continually work to fix these weaknesses, by releasing regular updates.

Using the latest versions of software, apps and operating system immediately improves your security.

Update regularly, or **set your phone or tablet to automatically update.**

That way you don't have to think about it.



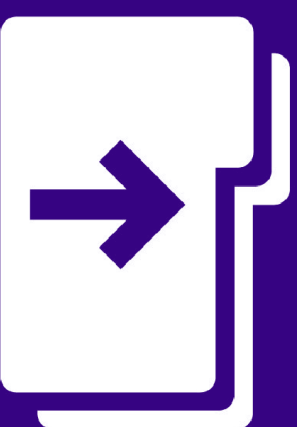
# #6 Turn on Backup |

## Turn on Backup

If your phone, tablet or laptop is hacked, your sensitive personal data could be lost, damaged or stolen.

Keep a copy of all your important information by backing it up.

You can back up all your data or only information that is important to you.



# PHISHING SCAMS

## Dealing with suspicious emails and text messages

# Phishing Scams

## Spotting suspicious messages

Spotting phishing emails and messages is becoming increasingly difficult. Many scams can even fool the experts. However, there are things to look out for:

**Authority**  
**Urgency**  
**Emotion**  
**Scarcity**  
**Current events**

If you're suspicious, there are steps you can take.

**Don't use links** or contact details in the message you have been sent or given over the phone.

**Use contact details you can trust:** visit the official website, call their advertised number, or log in to your account.

Most organisations will outline the things they will **never ask of you** – check if you are being asked for something on this list.

Further guidance on phishing attacks can be found here: [www.ncsc.gov.uk/guidance/suspicious-email-actions](https://www.ncsc.gov.uk/guidance/suspicious-email-actions)

# Phishing Scams

## Reporting suspicious messages

If you are suspicious of an email, report it by forwarding it to:  
**[report@phishing.gov.uk](mailto:report@phishing.gov.uk)**

If you are suspicious of a text, report it by forwarding it to:  
**7726**

You'll be helping protect others from being scammed.

# WHERE TO GET HELP & REPORTING

## ❑ Cyber Aware

- <https://www.ncsc.gov.uk/cyberaware/home>
- Advice from the National Cyber Security Centre

## ❑ Action Fraud

- [www.actionfraud.co.uk](http://www.actionfraud.co.uk)

## ❑ Reporting Phishing

- Suspicious Email Reporting Service (SERS)
- [report@phishing.gov.uk](mailto:report@phishing.gov.uk)



# THANK YOU!

❑ Any questions?

## Get in touch

Cyber Protect Officers - Lee Stripe &  
Kieran Hall

[DIU@Wiltshire.police.uk](mailto:DIU@Wiltshire.police.uk)

❑ **Feedback**

- <https://www.smartsurvey.co.uk/s/Individual-Wiltshire2021/>

