



# Cyber Crime





# Overview

Role of cyber crime unit

Types of cyber crime and cyber criminals

Prevent agenda

How cyber criminals access your accounts

Cyber crime prevention





# Cyber crime facts

£27 billion - Cost to UK of cyber attacks

£10.5 trillion - Cost worldwide by 2025

Cyber attack every 39 seconds

National priority status





# Cyber enabled crime

Traditional crimes, which can be increased in their scale or reach by use of computers, computer networks or other forms of information communications technology (ICT) – fraud/ grooming/ indecent images etc





# Cyber dependent crime

**Can only be committed using a computer; -**

**Hacking** - unauthorised access

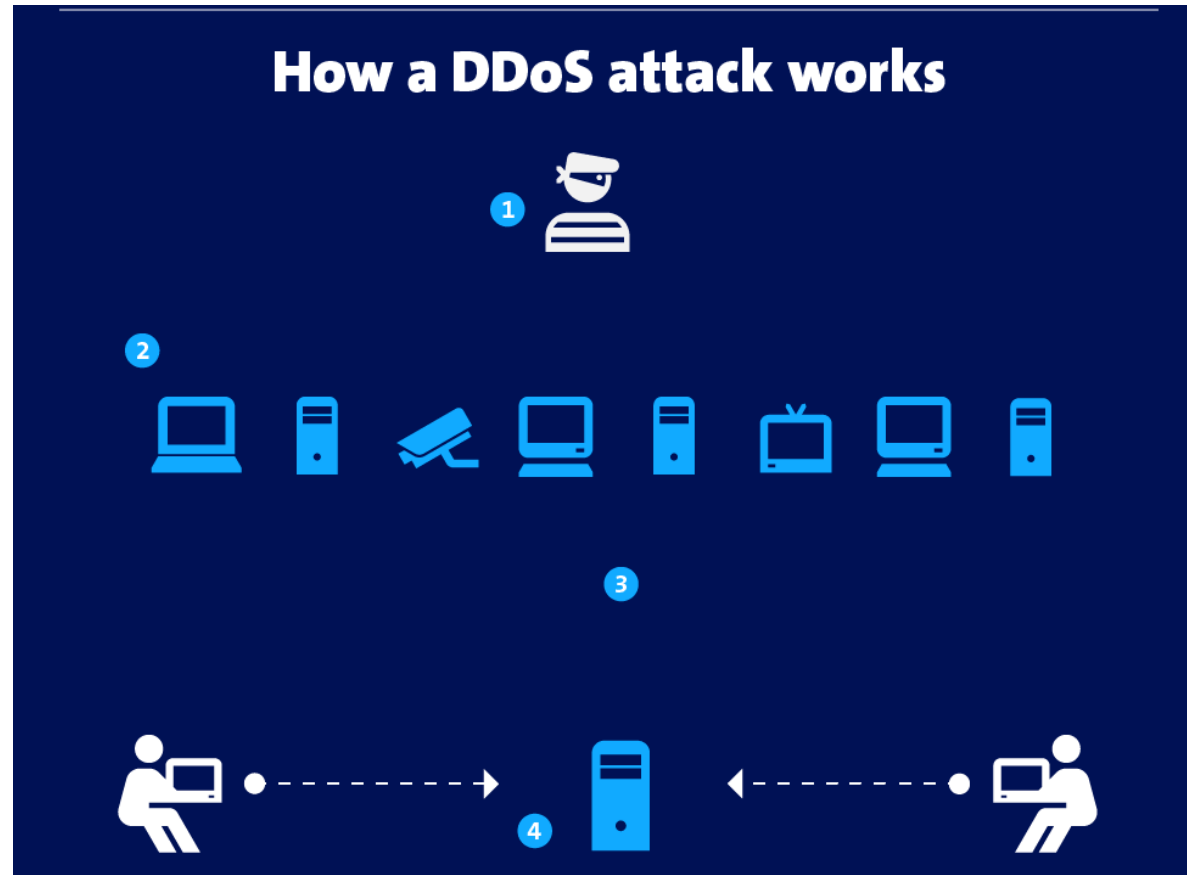
**Malicious software/ Malware** - can be spread between devices causing system crashes/deletion of files, or used to steal personal data. Viruses, worms, Trojans, spyware and ransomware are all types of malware.





# Cyber dependent crime

**Distributed Denial-of-Service (DDoS) attacks** - thousands of IP addresses are used to flood an internet server with so many requests that they are unable to respond quickly enough. This can cause a server to become overloaded and freeze or crash, making websites and web-based services unavailable.





# Cyber crime Unit

Only deal with cyber dependent crime  
- Computer Misuse Act offences

Investigate, provide prevention advice  
and work with offenders

Cyber dependent crimes are reported  
to Action Fraud and then disseminated  
to local police forces



**ActionFraud**  
National Fraud & Cyber Crime Reporting Centre  
0300 123 2040

**Unauthorised access to computer material**

-You watch your friend enter their username and password. You remember their login details and without their permission, login and read their messages

**2 years  
imprisonment  
or FINE**

**Unauthorised access with intent to commit another offence**

Your friend leaves their tablet on the sofa logged in to online banking and you transfer money from their account to yours .

**5 years  
imprisonment  
OR FINE**

**Unauthorised access with intent to impar or reckless to impair a computer**

You are playing an online game with a friend and are losing. You use a “booter” to knock them offline. **(Ddos)**

**10 years  
imprisonment**



**Unauthorised acts causing or creating serious risk of danger** - You hack a phone company and it stops people phoning 999. Your hack stops people being able to phone for an ambulance

**Life  
imprisonment**

**Making supplying or obtaining articles for use in other CMA offences** - You download software to bypass login details to hack a school computer but you haven't used it yet

**2 years  
imprisonment**



# Threat actors

**Script Kiddies** - less experienced hacker using existing software to commit attacks

**Insider threats** – Employee or former employee

**Hacktivism** - Politically or social change motivated

**Organised crime groups** - Professional group of cyber criminals, usually financially motivated and based abroad

**Advanced Persistent Threats** - Typically state sponsored, financially or politically motivated





# Prevent agenda

National Crime Agency predict UK based OCGs will turn to cyber-crime - low risk and high reward - little skill required

Exploitation -Grooming people to commit CMA offences

Age at first arrest for cyber crime is 17 years old





# Prevent agenda

Educate what constitutes a CMA offence

Work with agencies to identify people at risk of committing cyber-crime or who have committed an offence and work with them to divert away from cyber-crime

Disposal options - education visits  
cease and desist notices  
diversionary activities





# Protecting your accounts





# Data breaches

https://haveibeenpwned.com

Home Notify me Domain search Who's been pwned Passwords API About Donate

;-have i been pwned?

Check if your email or phone is in a data breach

email or phone (international format) pwned?





# Data breaches

## Breaches you were pwned in

A "breach" is an incident where data has been unintentionally exposed to the public. Using the [1Password password manager](#) helps you ensure all your passwords are strong and unique such that a breach of one service doesn't put your other services at risk.



**MyFitnessPal:** In February 2018, the diet and exercise service [MyFitnessPal](#) suffered a data breach. The incident exposed 144 million unique email addresses alongside usernames, IP addresses and passwords stored as SHA-1 and bcrypt hashes (the former for earlier accounts, the latter for newer accounts). In 2019, [the data appeared listed for sale on a dark web marketplace](#) (along with several other large breaches) and subsequently began circulating more broadly. The data was provided to HIBP by a source who requested it to be attributed to "BenjaminBlue@exploit.im".

**Compromised data:** Email addresses, IP addresses, Passwords, Usernames



**Onliner Spambot (spam list):** In August 2017, a spambot by the name of [Onliner Spambot](#) was identified by security researcher [Benkow moxu3q](#). The malicious software contained a server-based component located on an IP address in the Netherlands which exposed a large number of files containing personal information. In total, there were 711 million unique email addresses, many of which were also accompanied by corresponding passwords. A full write-up on what data was found is in the blog post titled [Inside the Massive 711 Million Record Onliner Spambot Dump](#).

**Compromised data:** Email addresses, Passwords





# Phishing

Phishing can be conducted via a text message, social media, phone call or email. .

Designed to trick receiver in to doing the “wrong thing”

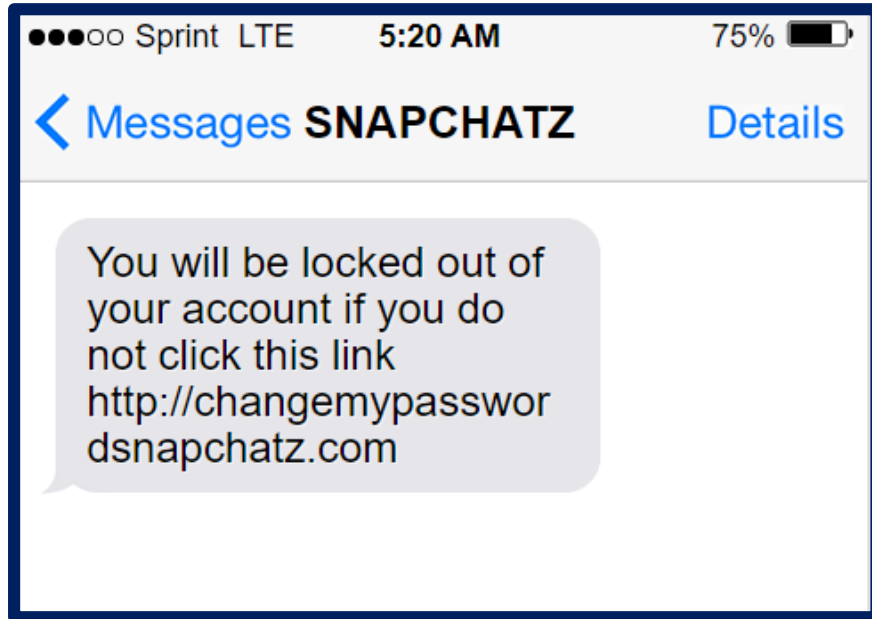
Intended to get you to reveal passwords, click on malicious links or pay money.







# Phishing



# Phishing

Go back to something you can trust such to verify information – visit the official website, log in to your account or ring the official number. Do not use the links or information sent in the email





# Passwords

Strong and separate password for email and other important online accounts

Create strong passwords using 3 random words

Save passwords in to browser or password manager





# Passwords

**Use strong and separate passwords for your email and other important accounts**

Reusing the same password for everything means puts all your accounts at risk if your data has been leaked

Your email is the hub that connects all other accounts together. If a hacker gets in to that, they can reset your passwords for other accounts using the forgotten password feature





# Passwords

Use 3 random words as commonly used passwords appear on password lists

Top 30 Most Used Passwords in the World		
1	123456	21 princess
2	password	22 letmein
3	123456789	23 654321
4	12345	24 monkey
5	12345678	25 27653
6	qwerty	26 1qaz2wsx
7	1234567	27 123321
8	111111	28 qwertyuiop
9	1234567890	29 superman
10	123123	30 asdfghjkl





# Passwords

Hackers use password crackers to brute force passwords - using a 12 character passwords with upper and lowercase letters would take 24 years to crack



## TIME IT TAKES A HACKER TO BRUTE FORCE YOUR PASSWORD IN 2022

Number of Characters	Numbers Only	Lowercase Letters	Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters, Symbols
4	Instantly	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	Instantly	Instantly	Instantly
6	Instantly	Instantly	Instantly	Instantly	Instantly
7	Instantly	Instantly	2 secs	7 secs	31 secs
8	Instantly	Instantly	2 mins	7 mins	39 mins
9	Instantly	10 secs	1 hour	7 hours	2 days
10	Instantly	4 mins	3 days	3 weeks	5 months
11	Instantly	2 hours	5 months	3 years	34 years
12	2 secs	2 days	24 years	200 years	3k years
13	19 secs	2 months	1k years	12k years	202k years
14	3 mins	4 years	64k years	750k years	16m years
15	32 mins	100 years	3m years	46m years	1bn years
16	5 hours	3k years	173m years	3bn years	92bn years
17	2 days	69k years	9bn years	179bn years	7tn years
18	3 weeks	2m years	467bn years	11tn years	438tn years



> Learn about our methodology at [hivesystems.io/password](https://hivesystems.io/password)



# Passwords

Save passwords in to a browser or use a password manager to avoid password overload

Turn on MFA and use strong passwords to protect your browser or password manager



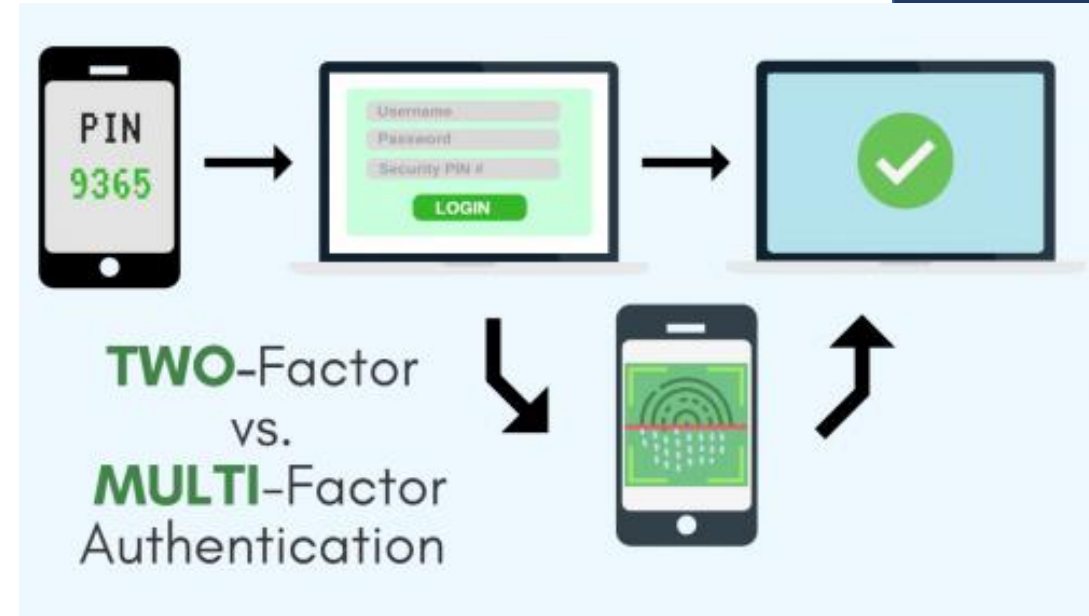


# Multi factor authentication

Turning on MFA will stop your account getting hacked, even if your password is leaked

Requires 2 or more pieces of identification to access your account

99% of hacked accounts did not have MFA turned on





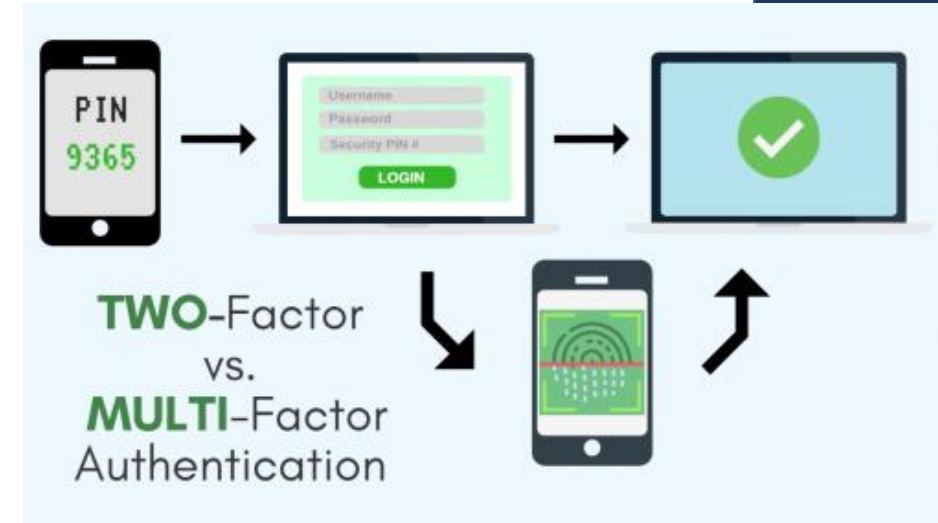


# Multi factor authentication

**Something you know** -  
password

**Something you have** - text with a  
code sent to your smartphone or  
other device, or a smartphone  
authenticator.

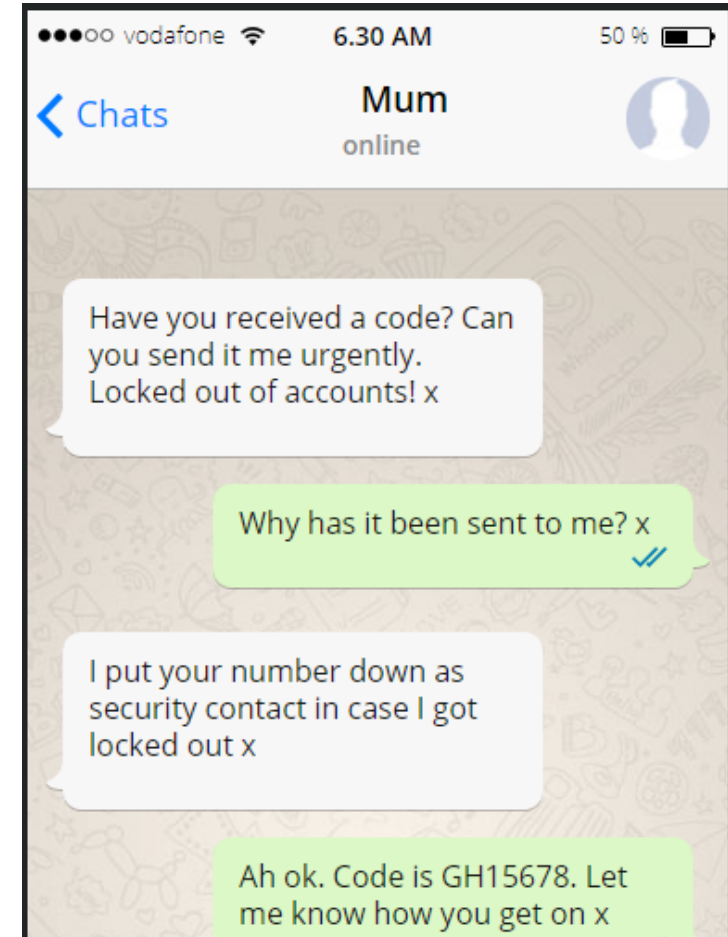
**Something you are** (biometrics  
using your fingerprint, face, or  
retina)





# Multi factor authentication

Do not share any one time codes or verification codes that have been sent to you, regardless of who has asked for them.





# Back up data

Back up any data that is important to you and save on to another device or cloud storage

Enable automatic back ups that will regularly save your information

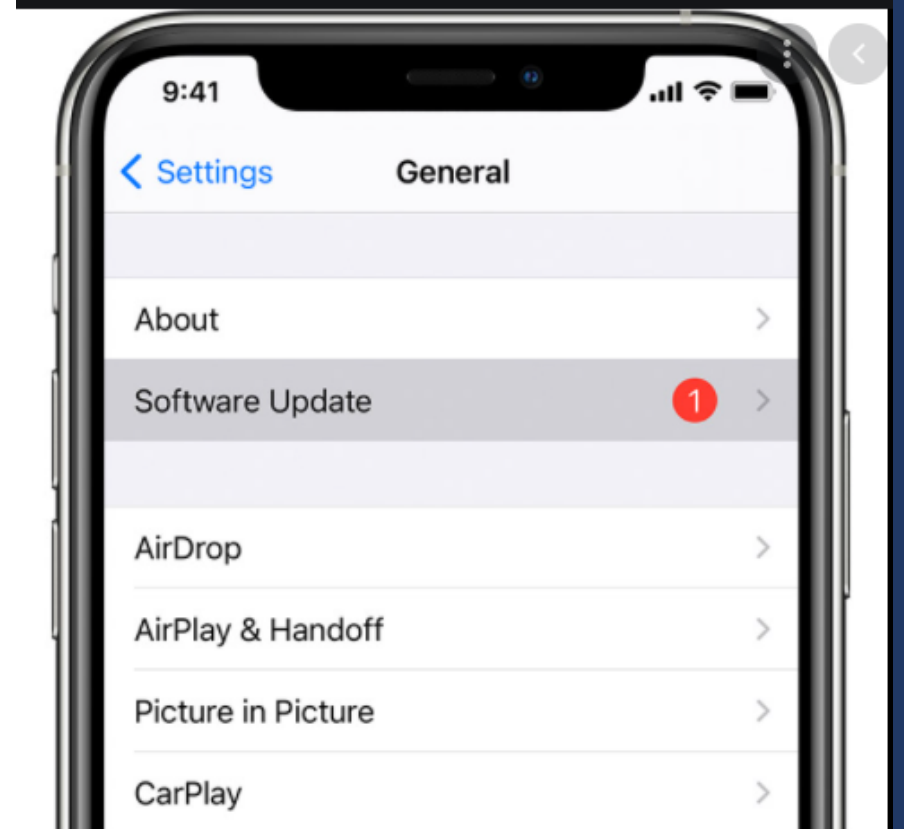
Disconnect external storage





# Update devices

Updating apps and software on your devices patches any known vulnerabilities





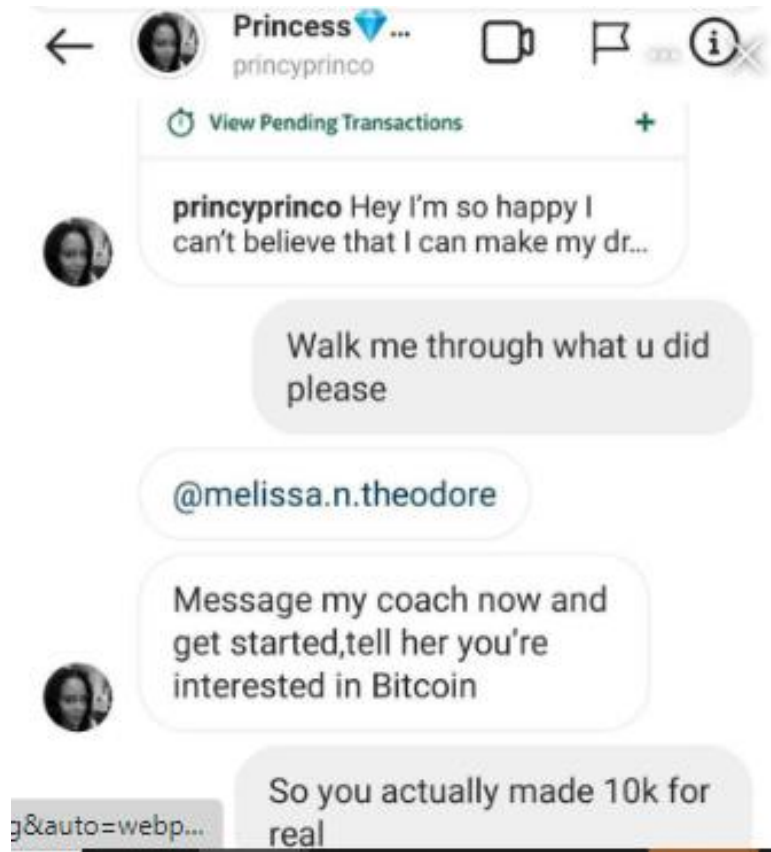
# Oversharing data

Think carefully before revealing personal information – could this be used to bypass security?





# Current scams.....





# Current scams.....

**ofgem**

## You Are Eligible To Apply For Energy Bill Rebate

Starting today the Government has announced an energy bill rebate scheme

**You have to apply for energy bill rebate before June 01 2022**

The government has announced a package of support to help households with rising energy bills. We will start making the payments in June 2022.

• This includes:

A £200 discount on their energy bill this Autumn for domestic electricity customers.

A £250 non-repayable Council Tax Rebate payment for all households that are liable for Council Tax.

Payment will be processed straight into your bank account

**How do I apply for energy bill rebate?**

You can get your rebate via Ofgem portal by clicking the button below:

[Claim Bill Rebate Now](#)

**SCAM**





# Keywords

Booters/ Stressers

Keyloggers

Hacking forums

Brute force

Denial of service

Distributed denial of service

Ddos panels







Questions???





# Contact

[CCU@lancashire.police.uk](mailto:CCU@lancashire.police.uk)





# Help and advice



National Cyber  
Security Centre  
a part of GCHQ

[ncsc.gov.uk](https://ncsc.gov.uk)



<https://cybergriffin.police.uk>



**ActionFraud**  
National Fraud & Cyber Crime Reporting Centre  
0300 123 2040