National Fraud Intelligence Bureau

CITY OF LONDON POLICE

ActionFraud
National Fraud & Cyber Crime Reporting Centre
0300 123 2040

# Cyber Threats and Crime Reporting in the UK

# Cyber Crime

## Cyber *Dependent* Crime under the Computer Misuse Act 1990

**Section 1:** Unauthorised access to or modification of computer material (website defacement, Ransomware)

**Section 2:** Unauthorised access to computer to facilitate the commission of an offence (Hacking etc)

**Section 3:** Unauthorised acts with intent to impair, or with recklessness as to impairing the operation of a computer – DDoS etc

# Fraud

## Cyber *Enabled* Crime under the Fraud Act 2006

# National Fraud and Cyber Crime Reporting Centre

ActionFraud
National Fraud & Cyber Crime Reporting Centre
0300 123 2040

## 0300 123 2040

Report fraud and cyber crime.
Help, support and advice.

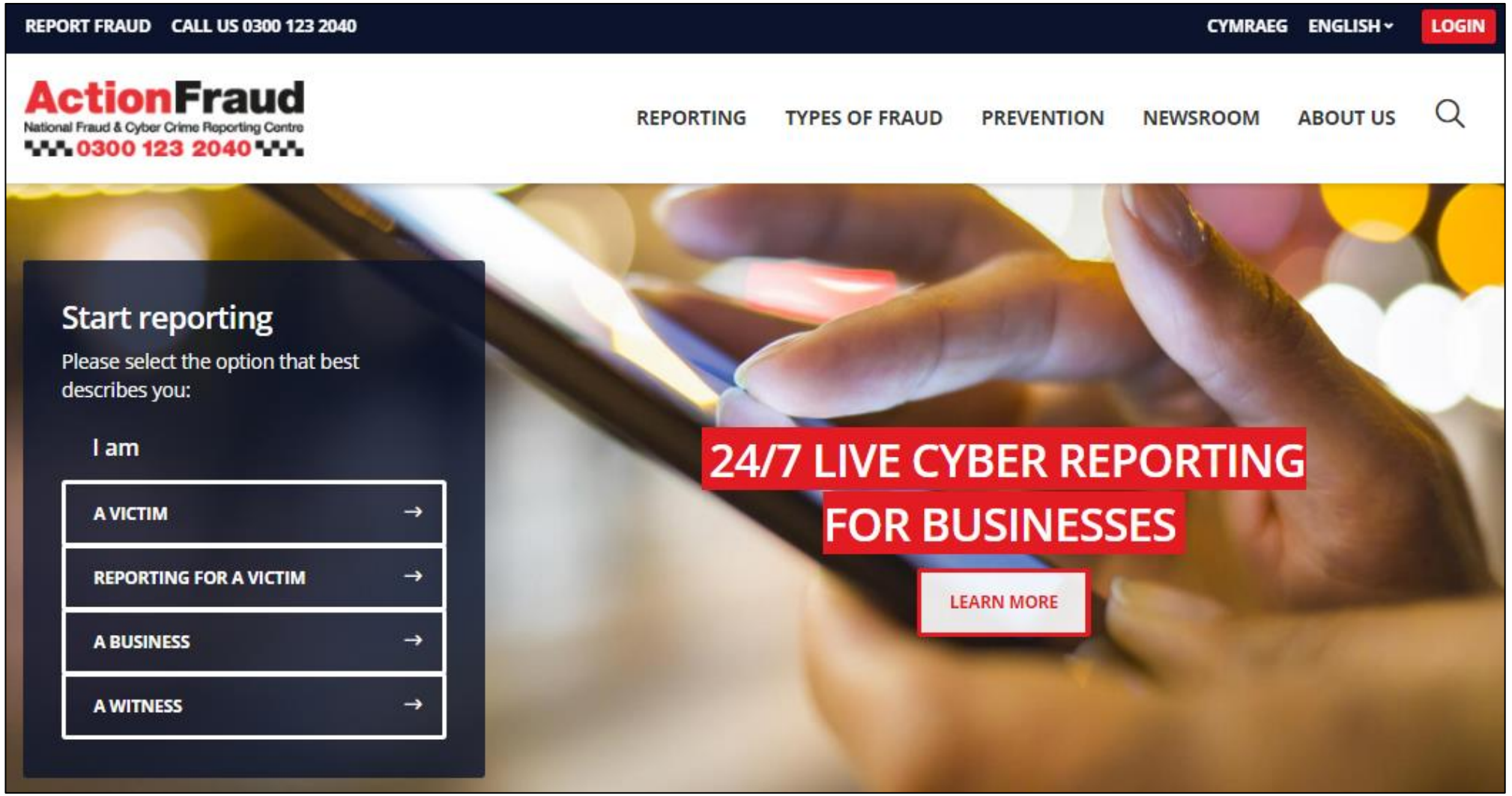
## Report 24/7 & Web Chat

**www.actionfraud.police.uk**
Secure online reporting.
News and Alerts.
Advice on avoiding the latest scams.

## 24/7 Live cyber

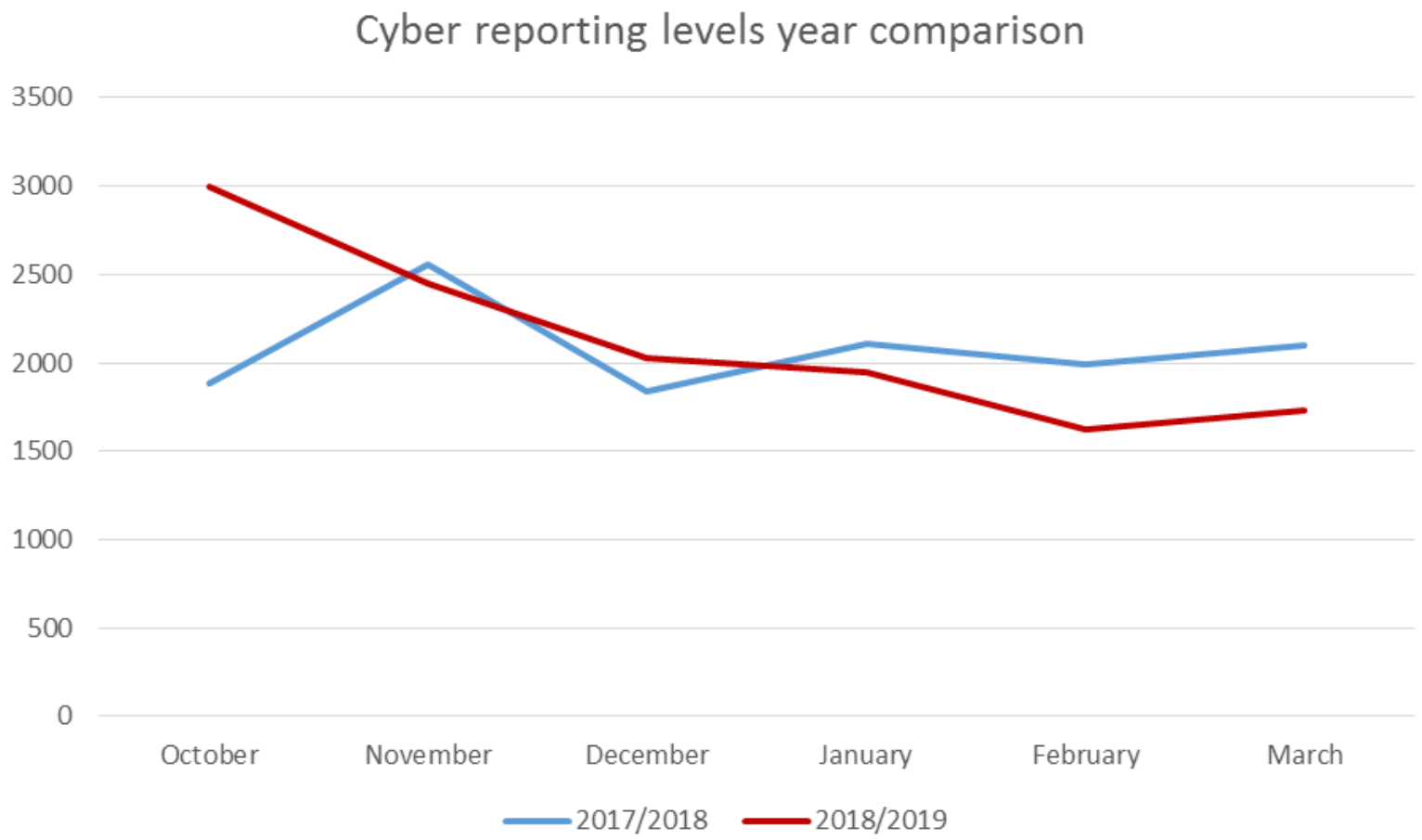
Specialist line for business, charities or organisations suffering live cyber attacks

# Online Reporting




https://www.actionfraud.police.uk/

# 6 Month Reporting Levels

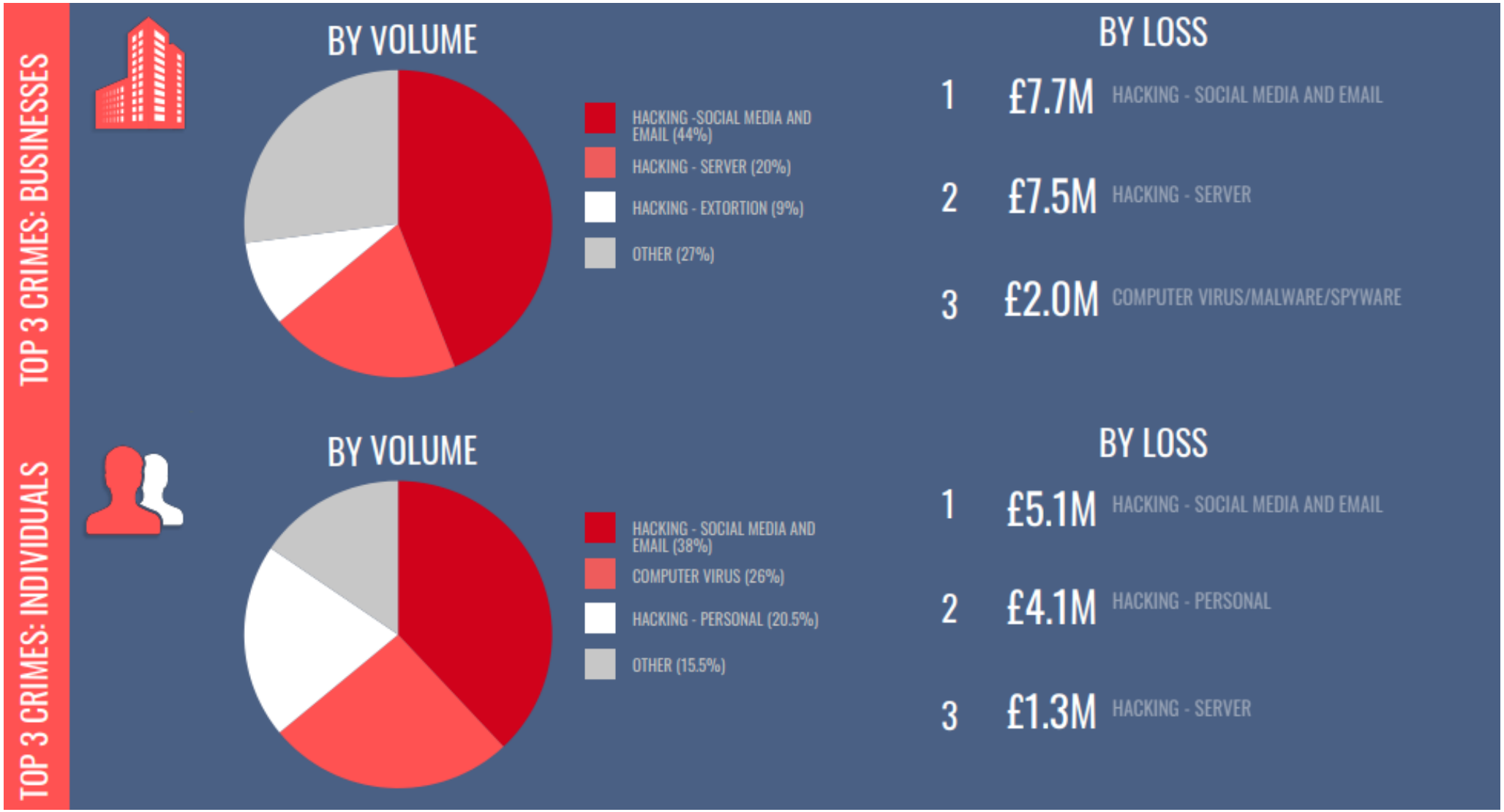



October 2017 – March 2018: 12,472

October 2019 – March 2019: 12,779

Overall, 16% reporting from business and 82% from individuals

# Overview in Trends and Threats



# Key Threats Facing the UK

- Ransomware

So far in 2018, Dharma/Crysis has been the most regularly reported strain (out of the hundreds of known strains)

2017 saw multiple high profile ransomware attacks hit the media including Wannacry, NotPetya (not strictly speaking ransomware) and Bad Rabbit

- Financial Trojans

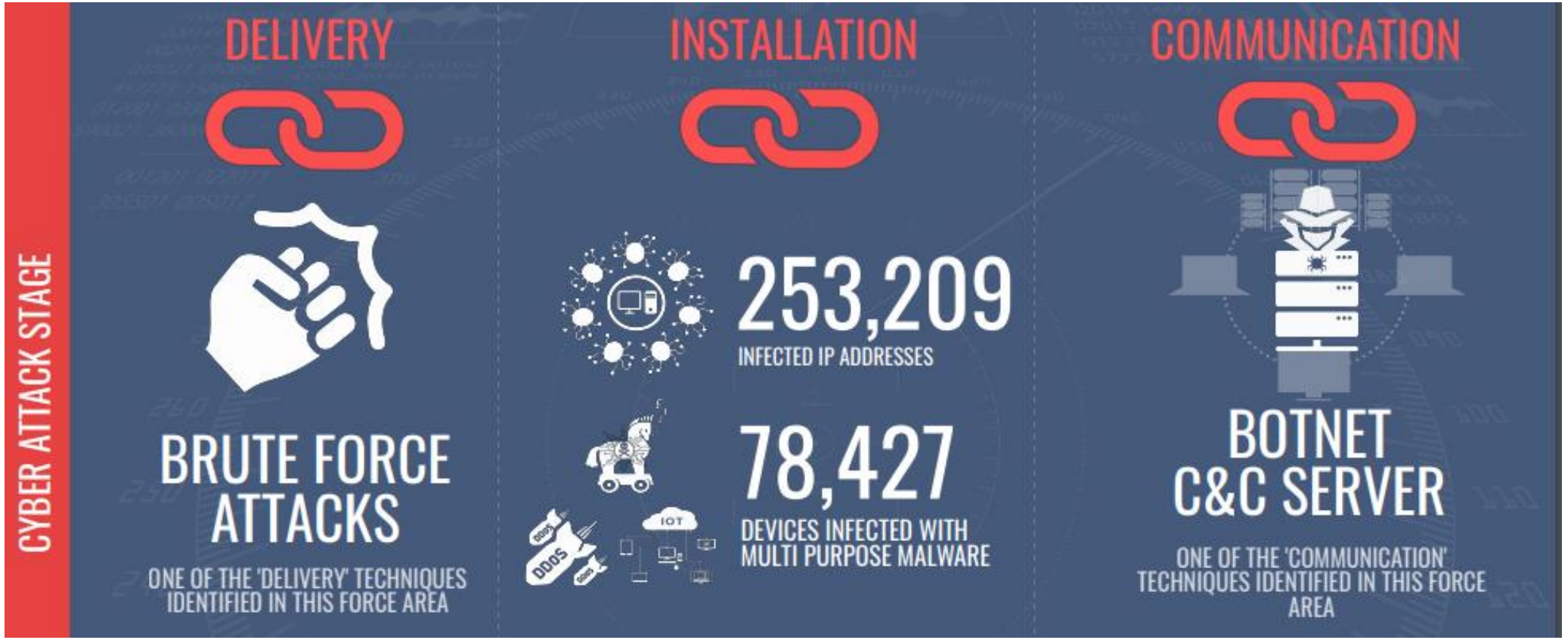
- DDoS Attacks

Some decrease in volume of reports but increase on severity of attacks. Financial organisations and government are seen as ripe targets by those primarily seeking to cause reputational damage.

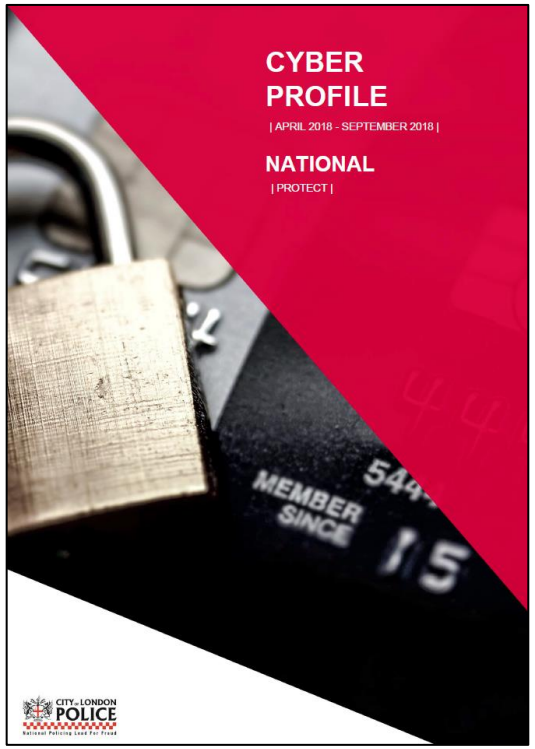
DDoS services are being offered for hire on the dark web

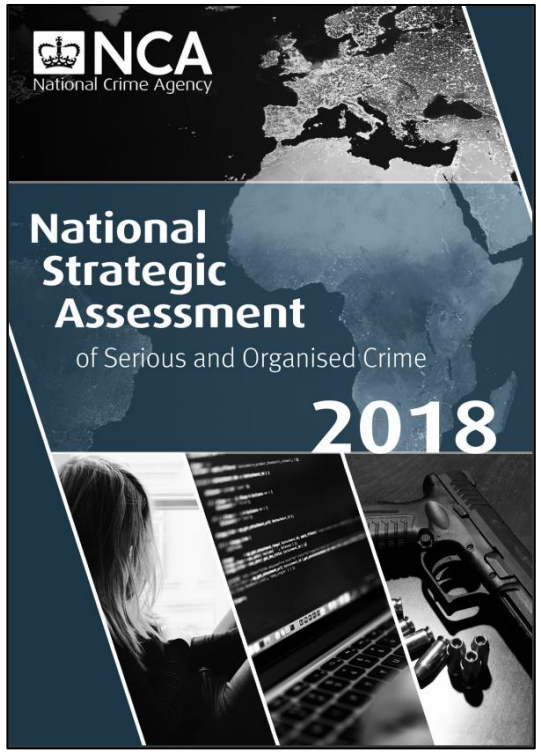
- Data Breaches

# Overview in Trends and Threats



# National Threat Assessments





CITY OF LONDON POLICE

NCA
National Crime Agency

National Cyber
Security Centre
a part of GCHQ

ico.
Information Commissioner's Office

# Public Awareness and Protection


Reproduced by kind permission of The Metropolitan Police Service's FALCON (Fraud and Linked Crime Online) team.

CYBER SCAMS

## PROTECTION FROM DDOS ATTACKS

### Know the signs of an active attack

Identifying that a DDoS attack is occurring allows for mitigation to be implemented at the earliest opportunity. The following symptoms could indicate a DDoS attack on your network:

- Unusually slow network performance (opening files or accessing websites)
- Unavailability of a particular website
- Inability to access any website
- A dramatic increase in the number of spam emails received

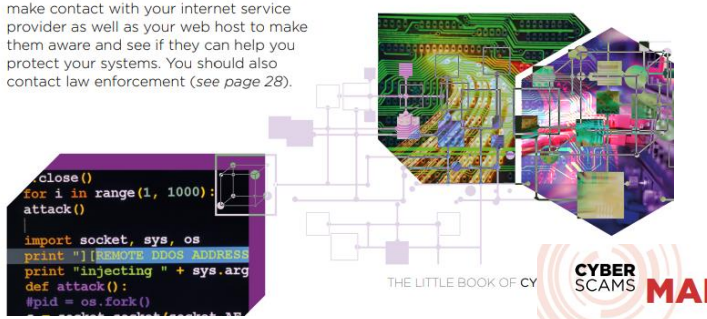
If an active attack is occurring you should make contact with your internet service provider as well as your web host to make them aware and see if they can help you protect your systems. You should also contact law enforcement (*see page 28*).

### Invest in DDoS mitigation

There are numerous different DDoS mitigation applications available from various suppliers. These work by analysing data traffic and identifying rogue traffic which is then not allowed to reach the victim server.

### DDoS extortion

If you are the victim of a DDoS extortion do not pay any demands. Retain any emails sent by the cyber criminal and report the incident directly to law enforcement *(see page 28)*.






CYBER SCAMS

## MALWARE

**The term malware refers to malicious software. This is software that is designed to gain unauthorised access to computers or other connected devices, disrupt their normal operation or gather information from them.**

Malware can infect a computer or network from a number of sources including:

- Contaminated email attachments.
- Infected websites, whether visiting directly or via links shown on emails or social media posts.
- From corrupt files stored on external devices such as laptops, mobile telephones or USB sticks, that are attached to the network.

### Common types of malware

**Spyware**

Spyware is designed to steal information about your activity on a computer or other device. Spyware can perform a number of functions including recording screen shots or logging keystrokes. This enables the criminal to obtain personal information that has been input in to a computer that they can then use themselves, such as internet banking passwords. Remote Access Trojans (RATs) are a type of spyware which allows a cyber criminal to remotely connect to infected devices and control them as if they were the authorised user.

MALWARE CAN INFECT A COMPUTER OR NETWORK FROM A NUMBER OF SOURCES

# Public Awareness and Protection

*#phishyfridays*

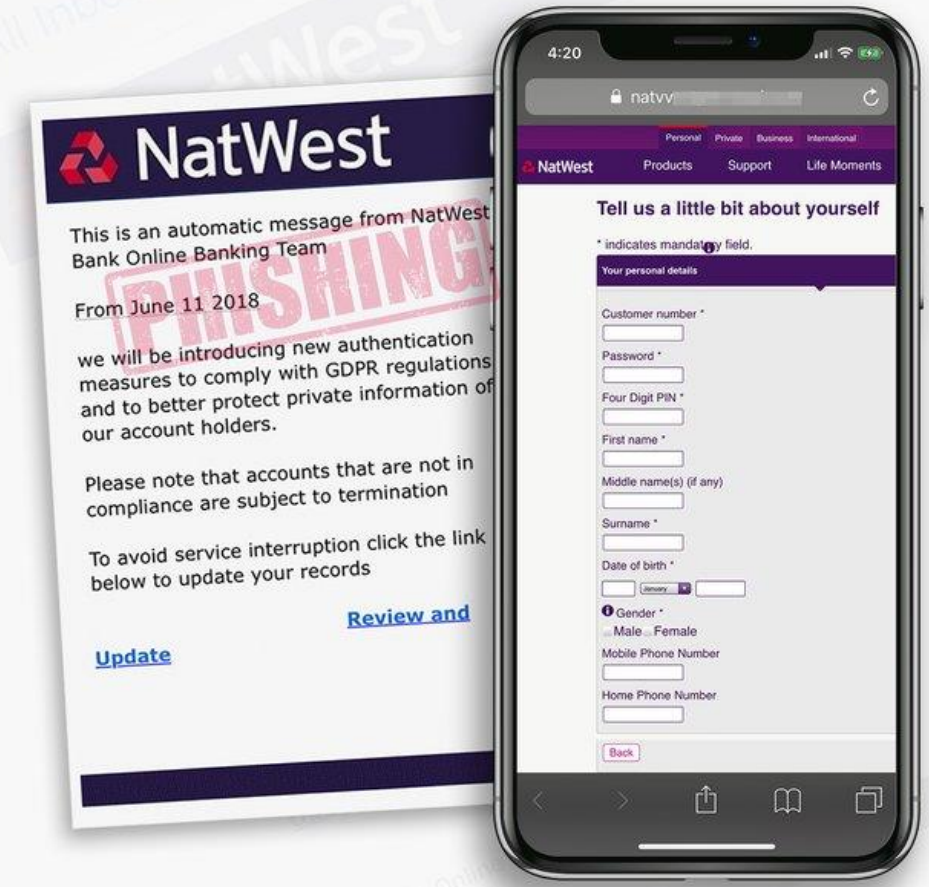
## Fake NatWest GDPR emails

This fake email purports to be from NatWest and claims that your account will be “terminated” if you don’t update your records. The “Review and Update” link in the email leads to a phishing website designed to steal personal and financial information.

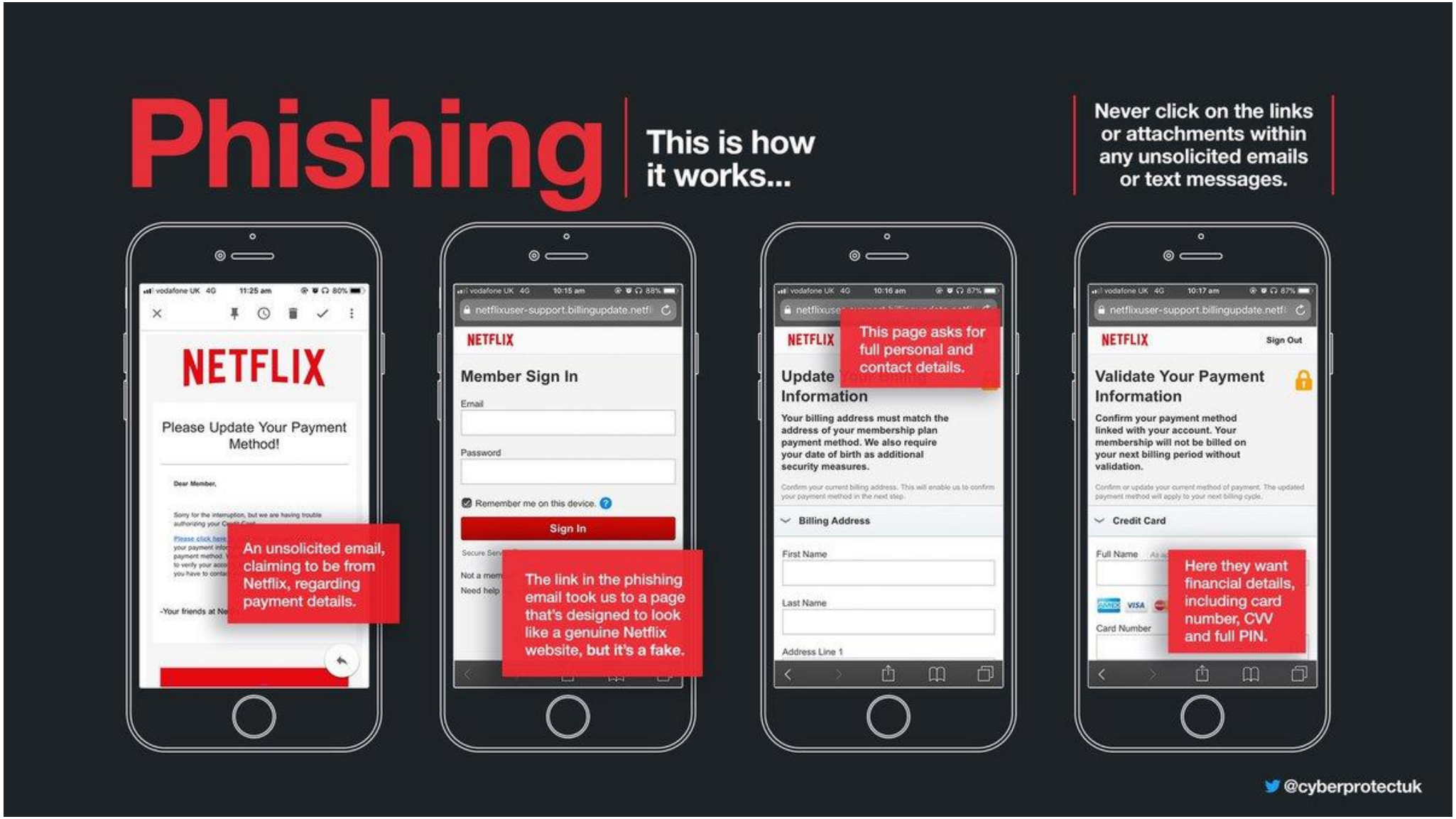
Don’t be tricked into giving a fraudster access to your personal or financial details. Never automatically click on a link or attachment in an unexpected email or text.

If you have been a victim of fraud or cyber crime, please report it to Action Fraud at Actionfraud.police.uk

CITY OF LONDON POLICE — ActionFraud National Fraud & Cyber Crime Reporting Centre actionfraud.police.uk — @cyberprotectuk



# Public Awareness and Protection



# Public Awareness and Protection

# Public Awareness and Protection

For more information about how to stay safe online, visit cyberaware.gov.uk

## STEP UP YOUR CYBER SECURITY GAME

## HERE'S HOW...


- **Lock down your email account.**

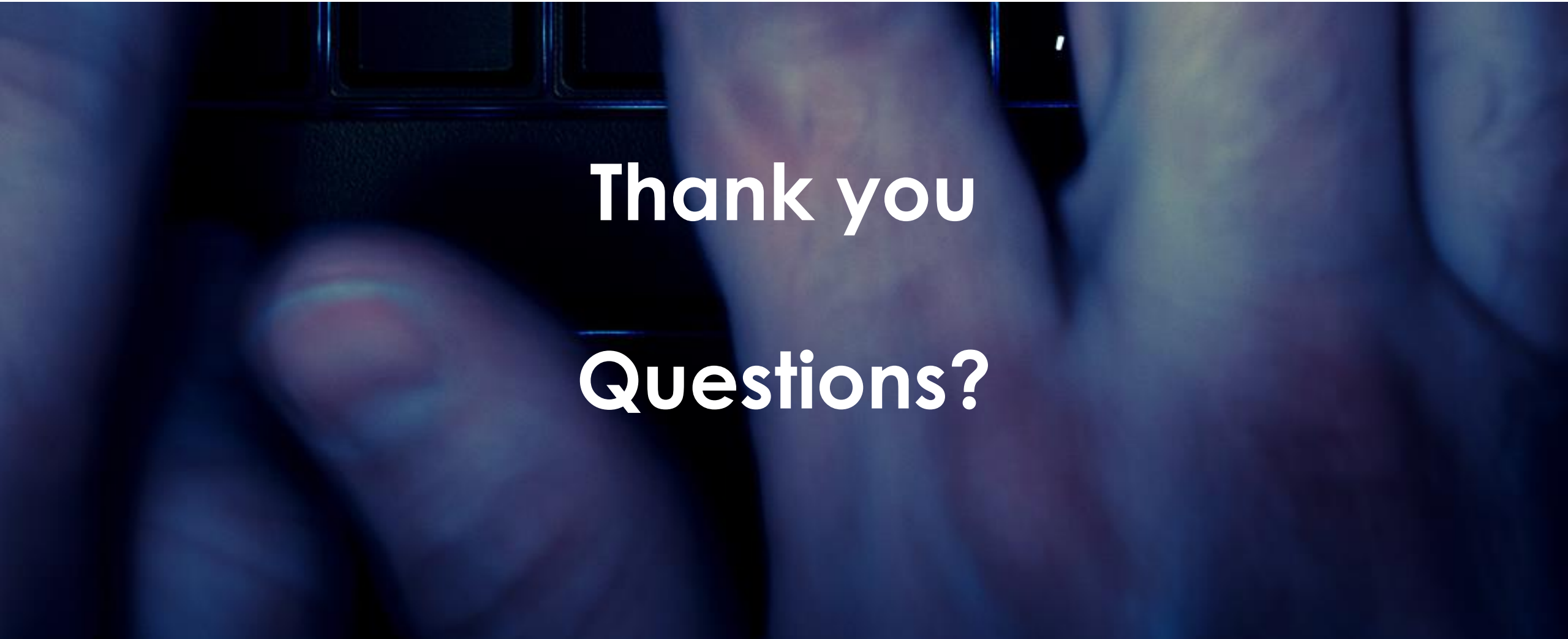
Cyber criminals can use your email to access many of your personal accounts and find out sensitive personal information, such as your bank details or home address. Protect your email account with a strong, separate password and 2FA.

CITY OF LONDON POLICE · ActionFraud National Fraud & Cyber Crime Reporting Centre actionfraud.police.uk · CYBER AWARE · @cyberprotectuk

National Fraud Intelligence Bureau

CITY OF LONDON POLICE

ActionFraud
National Fraud & Cyber Crime Reporting Centre
0300 123 2040



# Thank you

# Questions?