CYBER – SECURITY

PART 1

Keeping you safe in an electronic age

David Gibb, Cyber Protect Officer, Essex Police
Barry Linton, Thorpe Bay U3A

Criminal insight - why commit cybercrime?

VS

KENT POLICE ESSEX POLICE

Together reducing harm

scd

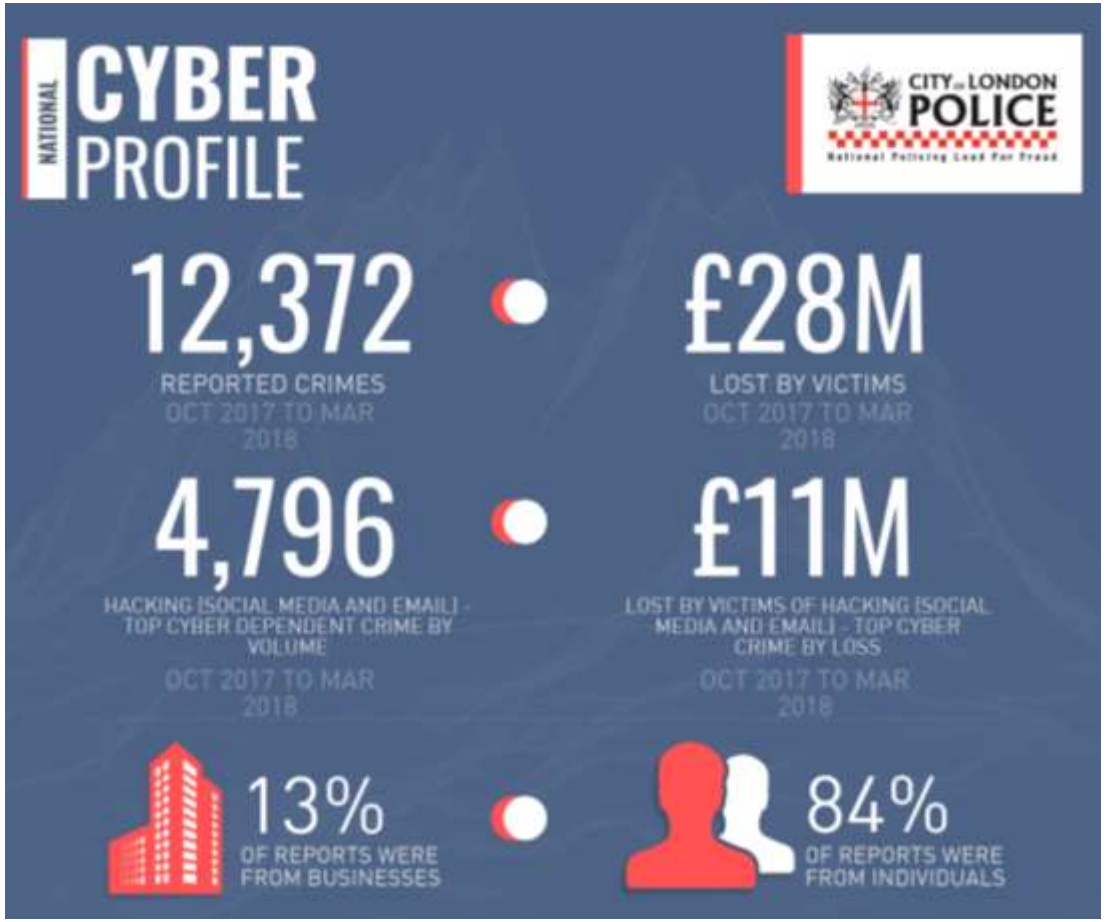
Serious Crime Directorate

Scale Nationally

- 1.6 million cyber crime incidents reported in the last year
- **£1,380 was the average loss for small businesses, the impact is not just financial.**
- **89% of small businesses also saw an impact on their reputation after an incident**
- Cyber related crime cost UK in excess of £130 billion in 2017
- **66% of small businesses had been a victim of cyber-crime**
- 1 in 10 people are a victim of cyber crime
- Reported Cyber and Cyber related crime up 9%

KENT POLICE ESSEX POLICE
Together reducing harm
scd
Serious Crime Directorate

Cyber National Profile



KENT POLICE ESSEX POLICE
Together reducing harm
scd
Serious Crime Directorate

Internet users in the UK: 2017

- In Quarter 1 (Jan to Mar) 2017, 89% of adults in the UK had recently used the internet (in the last 3 months), up from 88% in 2016; while 9% had never used the internet, down from 10% in 2016.

- Virtually all adults aged 16 to 34 years were recent internet users (99%), in contrast with 41% of adults aged 75 years and over.

- 90% of men and 88% of women were recent internet users, up from 89% and 86% in 2016.

- **Recent internet use among women aged 75 and over had almost trebled from 2011.**

KENT POLICE ESSEX POLICE
Together reducing harm
scd
Serious Crime Directorate

Current Biggest Threat Risk and Vulnerability

Demo

KENT POLICE ESSEX POLICE

Together reducing harm

scd
Serious Crime Directorate

What is currently the Biggest risk and vulnerability

KENT POLICE ESSEX POLICE
Together reducing harm
scd
Serious Crime Directorate

KENT POLICE ESSEX POLICE

Together reducing harm

scd
Serious Crime Directorate

I do not connect to Public Wi-Fi so I am safe

ARE YOU?

KENT POLICE ESSEX POLICE
Together reducing harm
scd
Serious Crime Directorate

CYBER - SECURITY

THE TARGETS….

Scope of Devices

WHAT DO THE “BAD GUYS” WANT

- Wreck your device – technical malice
- To know if your email address is live & used
- Grab your contacts list to further spread their malware
- Flood you and your contacts with many things
- Obtain your key identity information (aka Phishing)

- Ultimately – THEY WANT TO DEFRAUD YOU OF YOUR MONEY/GOODS!

HOW DOES THE MALWARE ENTER YOUR DEVICE?

- From Email Attachments
- From various Websites
- From files loaded from someone’s memory stick
- From remote scanning looking for open IP addresses

Phishing

MALWARE - VIA EMAIL ATTACHMENTS

Common attachment File Types:

.doc .docx .xls	Word documents and Excel spreadsheets
.pdf	document for printing
.jpg	photograph
.mpg .mov	movies (large files)
.wmv .mp3	sound/music
.zip	compressed file , need special software to open
.ppt or pps	Powerpoint Slides

These attachments could have embedded malware but most common Virus Protection software will find it.

BUT …

.exe	Executable Program	**DON'T OPEN IT!!**
.bat .scr	Process script	**DON'T OPEN IT!!**

MALWARE VIA WEBSITES

- Treat every website with caution, especially if a payment via your credit card is to be entered.
- Does the payment screen have
  //https: and a closed padlock symbol  showing in the browser URL bar at the top.
- Adult and dating websites.
  - Treat with extreme caution. They know if there is a problem you may be too embarrassed to deal with it.
  - Never allow such websites to have your personal and financial information, but remember they can see your IP address and hence approximate location.
  - Be very careful about allowing your photograph to be uploaded.
  - Remember the Ashley-Madison hack episode.
- Many such websites have registered domain names with one letter key shifted from well known websites
  - e.g. goggle.com, bcc.co.uk, marcsandspencer.com, whsmlth.co.uk

ON- LINE PURCHASES

- Particularly sites like eBay and Gumtree
- Look carefully at the photograph. Is it a stock advert photo.
  If it looks taken in the owners home, and shows the original box, the manual and all other bit and bobs, it is more reassuring.
- Do not mail off goods you sell without first receiving payment

AUTHORISED PUSH PAYMENTS (APPs)

Which Report Nov 2017

Banks are unlikely to refund if you are scammed in this way

- **'Malicious Misdirection' APP scams:**

When victims believe they are paying a known and legitimate payee but are instead tricked into making a push payment to a scammer's account. This can occur when you have been doing legitimate business with a company and may well be expecting a bill.

The bill arrives and looks authentic but unfortunately the recipient bank details are not.

- **'Malicious Payee' APP scams:**

When victims make a push payment, typically in return for promised goods or services, to people they believe are legitimate but who subsequently turn out to be scammers


“Your computer has a virus”
Computer Software Service Fraud
Fraudsters posing to be from legitimate companies, such as your Internet Service Provider (ISP) or Microsoft, claim that they will fix your computer for a fee. They may cold call you to offer this “service”, or create fraudulent websites, pop-ups and ads in order to lure you into calling them. What they’re really after is remote access to your computer and your financial details.
Never install any software, visit a website, reveal any personal or financial details as a result of a cold call or browser pop-up.
ActionFraud
CYBER AWAR
@CyberProtectUK

CALLS TO YOUR TELEPHONE

- “Microsoft have advised us they have detected some serious faults with your computer. We can fix it at a charge.”
- Nuisance marketing calls and text messages.
  - PPI
  - You have had an accident that was not your fault.
- New Laws in place from 1st October. You now need to opt-in to receive such messages, but the new laws have no control over calls from other countries.

- Calls from 0843 and 0844 numbers. Do not respond to a call-back message on your answerphone.
- Banks will **NEVER** phone you and ask you for your password or PIN number.
- Calls may show a regular UK landline number on your phone screen. This can be false.

TELEPHONE

- Enroll on Telephone Preference Service.

www.tpsonline.org.uk

- BT and other Telephone networks offer an answering intercept service.

  Your phone will not ring and the caller will be requested to give their name and the reason for the call. Only then will the call ring on your phone and you will hear the recorded message and decide whether or not to take it.


FAKE MY PHONE
Fake Caller ID
Call from a different number. Disguise your caller id, it's easy and works on any phone!
Try a Free Call
Get Started


Clockwork
Home
API Docs
Integrations and plugins
Pricing
FAQs
Blog
Support
Log in
Sign up
The Easy Text Message SMS API
Send and receive SMS through your app
Sign up for free

CORPORATE ATTACKS

- Large organizations have their databases hacked and private information about their clients is taken.
  - Talk Talk
  - Equifax
  - Ashley Madison
  - Possibly some NHS systems
  - Carphone Warehouse
- Denial of Service Attacks
- Corporate Ransomware
  - Their databases become virus encrypted and unusable until a ransom is paid.

  Should you read in the press about a company who may hold your data, **be additionally on your guard**.

CREDIT CARDS IN YOUR WALLET

- CLONING
  - Never let your card out of your hand. The machine must come to you. Be very suspicious of a machine that “doesn’t work”

- CONTACTLESS SKIMMING
  - RFID protective boxes or sleeves.
- If you need to call your bank, **use the phone number on your card**, not the one that may be given on a warning email or text message

CREDIT CARDS IN YOUR WALLET