

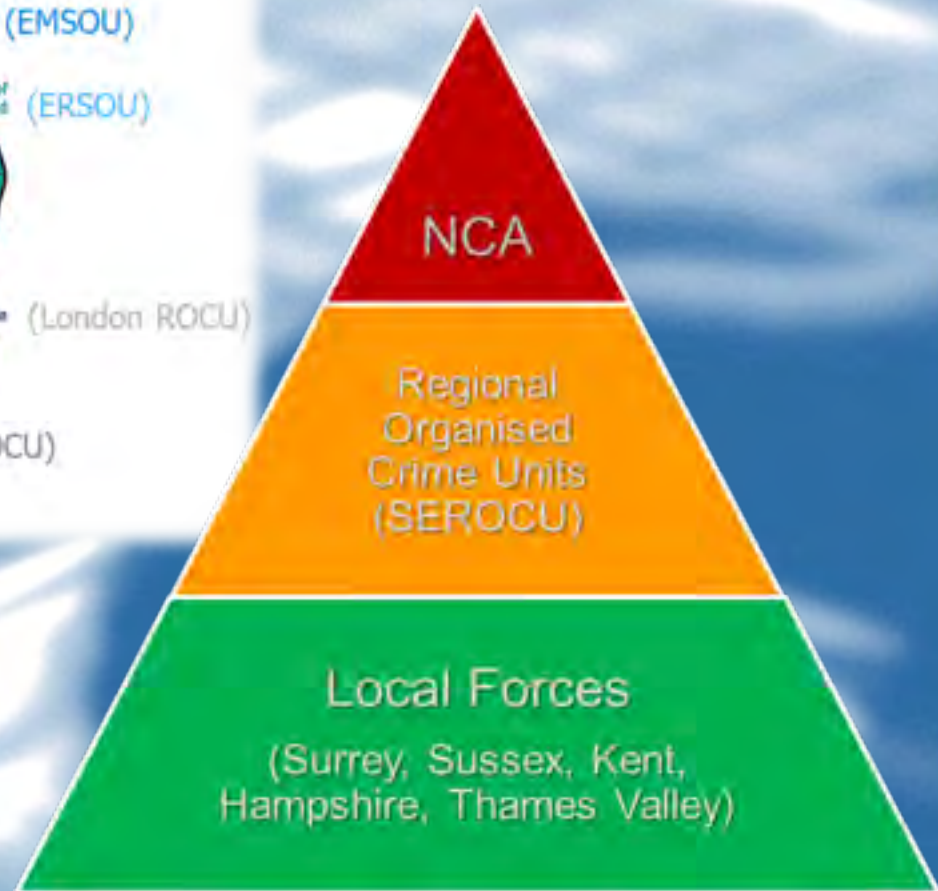
Introduction

Regional Cyber Protect Officer for SEROCU

To engage with, and develop relationships with companies and organisations within the region to promote cyber security and the role of the SEROCU CCU.



The Regional Units



Cyber Crime In Numbers

- 3.9 Million cyber crimes in 12 months (2016)
- 28% of businesses reported attacks to Police
- Cost to UK economy...
£27 Billion in 2011 → £49 Billion in 2014
- Average breach costs £65k to £115k (small company)
- 500 Million new viruses in 2015
- 3000 DDoS attacks per day
- 500K phishing attempts per day

Passwords



1. 123456
2. linkedin
3. password
4. 123456789
5. 12345678

- Password policy (repeat passwords)
- Educate staff not to use same ones as personal accounts

Passwords

HOW SECURE IS MY PASSWORD?

ENTER PASSWORD

Sponsored by [Dashlane](#): never forget another password

 Follow @hsimpnet

 Like 

Sponsored by [Dashlane Password Manager](#)

Top 10,000 passwords by [Mark Burnett](#) / Typefaces by [The League of Movable Type](#)

The [source code](#) for this site and the official HSIMP [jQuery plugin](#) can be found on [GitHub](#)

© [Small Hadron Collider](#), 2016 / Version 8.0

This site is for educational use. Due to limitations of the technology involved, the results cannot always be accurate. Your password will not be sent over the internet.

Password Security

Passwords

HOW SECURE IS MY PASSWORD?



It would take a computer about

2 QUATTUORDECILLION YEARS

to crack your password

Dashlane can help you remember all of your secure passwords - and it's free!

[Tweet Your Result](#)

TIP: USE A PASSWORD MANAGER TO SECURE AND EASILY REMEMBER YOUR PASSWORDS

"Dashlane is life changingly great. Get it!" - David Pogue (The New York Times)
Get Dashlane - It's Free!

LENGTH: LONG

Your password is over sixteen characters long.
Never forget your long, secure password by using a password manager

Powered by Dashlane. Never forget another password.

Have You Been Compromised?



Home

Notify me


Domain search

Who's been pwned

Pastes

API

About

Donate 

';--have i been pwned?

Check if you have an account that has been compromised in a data breach

pwned?

122

pwned websites

1,308,726,979

pwned accounts

37,747

pastes

29,634,108

paste accounts

[pwned?](#)

A Socially Engineered Story

The image illustrates a socially engineered story through a collage of social media and news snippets on the left, and a screenshot of the SPOOFTEL website on the right.

The collage on the left includes:

- A LinkedIn profile for Knight CF Xmas.
- A news article titled "The Judge" from the "comms aw" (communications awards).
- A LinkedIn profile for Matthew Yearwood, Director of Digital Corporate Finance at JPMorgan Chase & Co.
- Other snippets from "Just Give" and "ICAEW".

The SPOOFTEL website screenshot shows:

- Header: **SPOOFTEL** THE WORLD'S LEADER IN CALLER ID SPOOFING
- Navigation: Free Call, Rates, FAQ, Apps, Developers, Contact, Sign Up
- Main Content: **FREE CALLER ID SPOOFING TRIAL**
- Form Fields:
 - Your Number**: Input field with a dropdown menu (value: 3). Text below: "Enter the number you are calling from"
 - Destination Number**: Input field with a dropdown menu (value: 1). Text below: "Enter the number you would like to call"
 - Spoof Number**: Input field. Text below: "Enter the number you would like displayed"
 - Voice Pitch**: Slider control. Text below: "Adjust the pitch of your voice"
 - Soundboard**: Slider control. Text below: "None"
 - AARCEJ**: Input field. Text below: "Enter the Text Above"

Peel's First Principle

*"The basic mission for which the Police exist is to **prevent** crime and disorder"*



It Is Preventable!!

80%

...of cybercrime is preventable (GCHQ)

Becoming a Victim

How will you find out..?

- 1) The criminals themselves
- 2) An irate supplier/customer
- 3) The Police
- 4) Member of staff
- 5) The press
- 6) Internal computer software

7) You may never find out..

Ransomware

- Currently targeting individuals
→ Moving towards businesses

- Demands from £600+
- No guarantees to get data back
- Supporting criminality
- Repeat victimisation

- Backup using an external HDD
- Do it regularly
- Store backup securely
- Cloud storage not immune



WARNING!
Your personal files are encrypted!

11:59:04

Your documents, photos, databases and other important files have been encrypted with strongest encryption and unique key, generated for this computer. Private decryption key is stored on a secret Internet server and nobody can decrypt your files until you pay and obtain the private key. The server will eliminate the key after a time period specified in this window.

Open <http://maktub5bqjfsujt2.onion.link>
or <http://maktub5bqjfsujt2.torstorm.org>
or <http://maktub5bqjfsujt2.tor2web.org>

in your browser. They are public gates to the secret server.

If you have problems with gates, use direct connection:

1) Download TOR Browser from <http://torproject.org>
2) In the Tor Browser open the <http://maktub5bqjfsujt2.onion>

(Note that this server is available via Tor Browser only. Retry in 1 hour if site is not reachable).

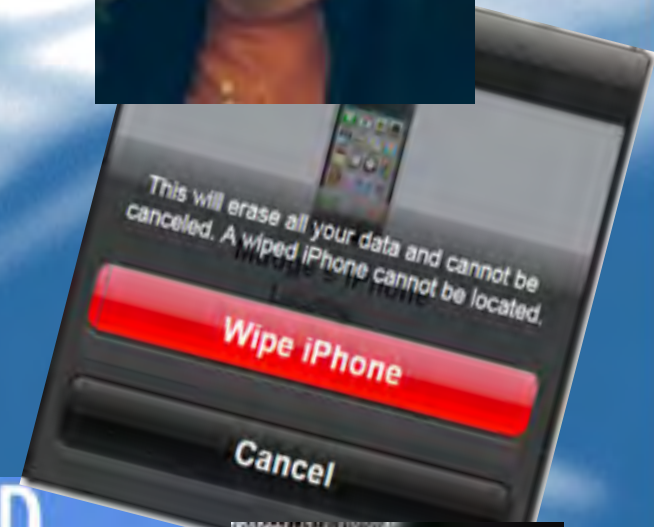
Write in the following public key in the input form on server:

```
m126-11598-r137-2296-2212-5215-1184-1584-1720-2210-1721-2208-1028-1732-  
2222-2192-2299-1713-1813-1415-1821-1821-1821-1821-1821-1821-1821-1821-1821-  
1821-1821-1821-1821-1821-1821-1821-1821-1821-1821-1821-1821-1821-1821-  
1821-1821-1821-1821-1821-1821-1821-1821-1821-1821-1821-1821-1821-1821-  
1821-1821-1821-1821-1821-1821-1821-1821-1821-1821-1821-1821-1821-1821-  
1821-1821-1821-1821-1821-1821-1821-1821-1821-1821-1821-1821-1821-1821-
```

Copy Public Key to Clipboard 

A Recent Investigation (Malicious Insider)

- Richard Neale sent a “Wipe Command” to 900+ Aviva employees devices - BYOD
- Further access and alterations made into companies systems
- Tried to hide his involvement by using VPN's but forensic investigation identified incriminating artefacts on his devices
- Cost the company £500K
- Convicted and serving 18 months



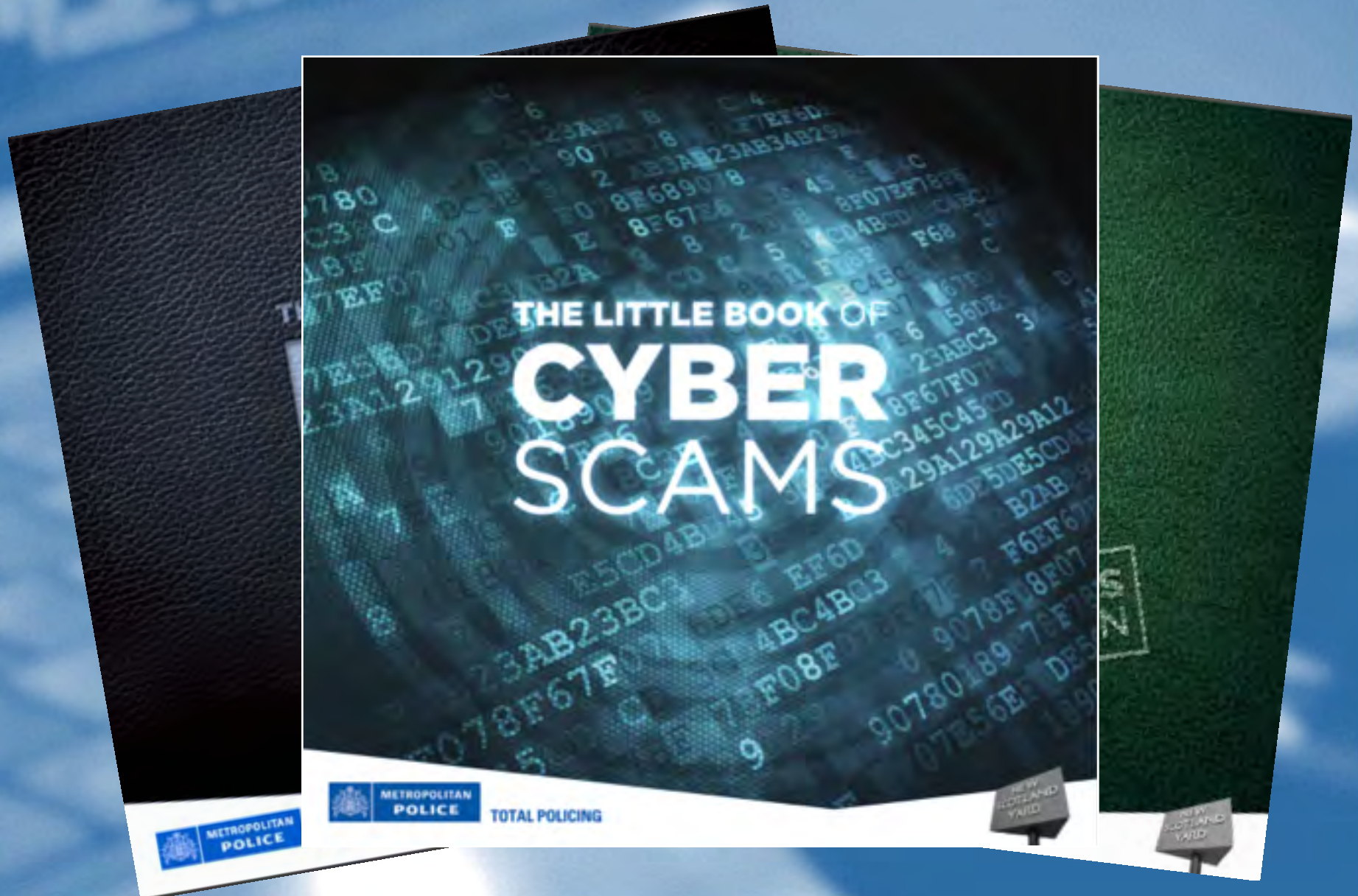
Cyber Essentials



1. Boundary firewalls and internet gateways
2. Secure configuration
3. Access control
4. Malware protection
5. Patch management



Free Stuff



General Data Protection Regulation



Fined £400k

Global Turnover £1.84b

**Possible
fines of
4%
of global
turnover
or €20M**

 Google Inc

20 August 2015, Enforcement notices, Online technology and telecoms

Action Fraud



Cyber-security Information Sharing Partnership

The image shows the homepage of the CERT-UK Cyber-Security Information Sharing Partnership (CSP). The header features the CERT-UK logo and the CSP logo, a search bar, and navigation links for Home, Contact, Members, Privacy, and Create. The main content area includes a featured article titled "Cyber-attacks: would your business get caught out?" with a sub-headline "Three scenarios CERT-UK repeatedly see targeting organisations as well as mitigation advice". Below this is a large graphic of a computer monitor displaying a grid of folders, with a red folder highlighted and a red padlock icon overlaid. Three red padlock icons are also scattered around the monitor. Below the graphic are three circular icons: a yellow one with a graph, a green one with an envelope, and a red one with a headset. Each icon has a corresponding text block: the yellow one says "Sign up for the CERT-UK Network Incident Response (NIR) services tailored to your organisation"; the green one says "Update your profile and set your preferences to receive email notifications to ensure you see the information you want"; and the red one says "Check in regularly to CERT-UK or visit our Support Pages for vital guidance". At the bottom, there are two sections: "What's Happening" with a "view feeds" link and a post titled "New Post ISO29147 - Vulnerability Disclosures - now free" by MartinMI (@objective); and "TLP Guide" with a table of information sharing levels.

CERT-UK CSP

Home Contact Members Privacy Create

Cyber-attacks: would your business get caught out?
Three scenarios CERT-UK repeatedly see targeting organisations as well as mitigation advice

Sign up for the CERT-UK Network Incident Response (NIR) services tailored to your organisation

Update your [profile](#) and set your [preferences](#) to receive email notifications to ensure you see the information you want

[Check in regularly](#) to CERT-UK or visit our [Support Pages](#) for vital guidance

What's Happening [view feeds](#)

New Post ISO29147 - Vulnerability Disclosures - now free*
by [MartinMI \(@objective\)](#)

TLP Guide

Max	Available to anyone
Green	Available to CSP community
Yellow	Available to invited members of CSP

Key Points

Easy take-aways..

- 1) Update your OS (Microsoft/Apple/etc)
- 2) Strong different passwords (consider 2FA)
- 3) Set AntiVirus to auto-update & scan
- 4) Disable macros in Microsoft Office
- 5) Control use of USB sockets
- 6) Administrator account control
- 7) Backup strategy
- 8) Upgrade any XP machines

9) EDUCATE YOUR STAFF!!

Thank You

DS Chris Greator

[@SouthEastROCU](#)

cyberprotect@serocu.pnn.police.uk