Information security

U3a Computer Support Group

October 2019

Henry Wallis

Cyber Security Awareness Month – October 2019

- Agenda
- Who? What? How?
- How to protect
- Where to go for help

NB - This is a “Henry personal” presentation, not one on behalf of my employer

A dialogue not a monologue

Information security ??

- Information security
- Cyber security
- Cyber resilience
- …..

Don’t really care what you call it – just need to make sure that you keep safe!!

What attacks? By whom?

- Theft
- Phishing
- Vishing/Smishing
- BEC

Phishing

- Email etc to get you to:
  - Provide bad guys with your credentials etc
  - Download keylogger
  - Download ransomware
  - Pay bad actor money / buy gift vouchers
- Something that gets your attention
  - You have won lottery
  - Due refund – HMRC/DVLA
  - Nigerian prince etc
  - From trusted person – police, boss etc

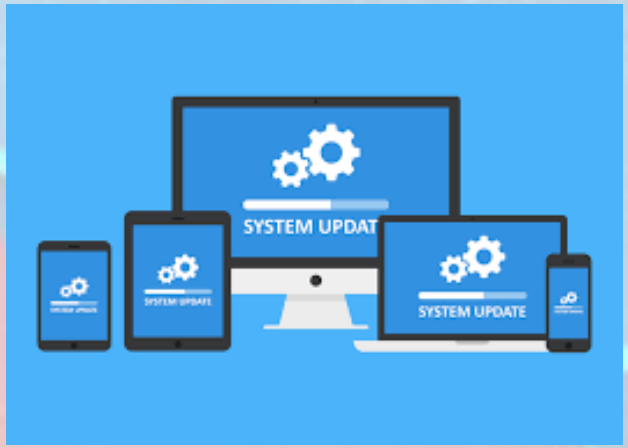
What attacks? By whom?

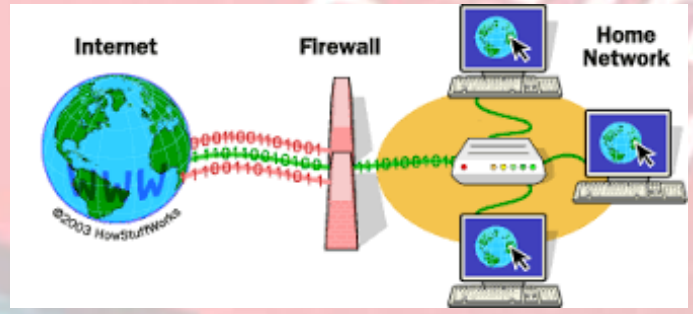
- Theft
- Phishing
- Vishing/Smishing
- BEC
- Deep fake
- Telephone calls
- Ransomware
- Waterhole attacks - wifi
- Drive-by

- Criminals
- Foreign gov’ts
- Hackers
- Political activists
- Terrorists
- Insiders
- Honest mistakes

Solutions (1)

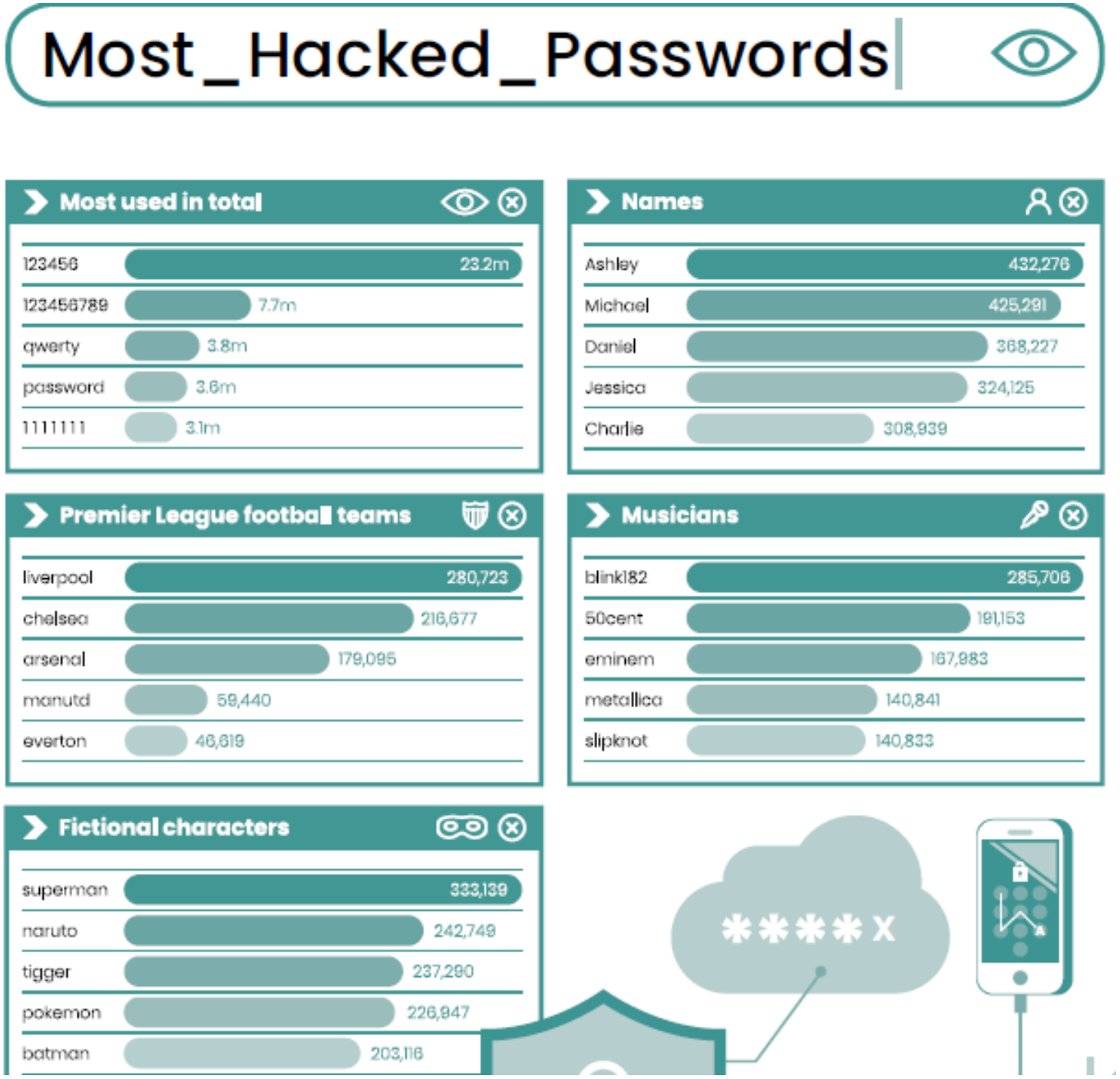
- Patching
  - Set phone/tablet to automatically install latest updates
- Anti-virus
  - Install and keep up to date
- Firewalls
  - Install and keep on
- System/device settings
  - Default?
- Back up
  - To a separate hard disk
  - To the cloud
  - Regularly
  - Check it works
  - Encrypt?





Solutions (2)

- Strong passwords / password manager


Most_Hacked_Passwords
Most used in total
123456 23.2m
123456789 7.7m
qwerty 3.8m
password 3.6m
1111111 3.1m
Names
Ashley 432,276
Michael 425,291
Daniel 368,227
Jessica 324,125
Charlie 308,939
Premier League football teams
liverpool 280,723
chelsea 216,677
arsenal 179,095
manutd 59,440
everton 46,619
Musicians
blink182 285,706
50cent 191,153
eminem 167,983
metallica 140,841
slipknot 140,833
Fictional characters
superman 333,139
naruto 242,749
tigger 237,290
pokemon 226,947
batman 203,116
*****X

Passwords

- https://haveibeenpwned.com
- Ideally separate password for each account ☺
  - At least for the key ones
- Strong password generator – https://passwordsgenerator.net/
- Combination of:
  - Upper case, lower case
  - Numbers
  - symbols
- Pass phrase – not password
  - 3 words
    - Blue Elephant Icing - becomes
    - Blu3Elephant1c!ng
  - 1st letters of phrase - Tqbfjotld

Password managers

- LastPass
- 1Password
- KeePass
- Dashlane
- Others are available!

- Most are free, with paid-for extras
- Able to use on any device

Solutions (2)

- Strong passwords / password manager
- 2FA / MFA

2/MFA

- SMS – one-time password
  - Can be compromised by sim hack
- Google/Microsoft Authenticator app
- Yubico security key/devices (others available!)

Solutions (2)

- Strong passwords / password manager
- 2FA / MFA
- Encryption
  - Scrambling of data so it can only be read with the appropriate key to unlock
  - Simple – A→B; B→C; C→D etc

Encryption

Hard disk

- Bitlocker – Windows 10
- TrueCrypt / Veracrypt

Data in transit

- https
  - A necessary for a secure site but not a guarantee

Solutions (2)

- Strong passwords / password manager
- 2FA / MFA
- Encryption
- Security awareness
  - Limit what you share
  - Putting your holiday on Facebook → house burgled??

The NCSC's advice for individuals and families

Protect your accounts…

- Use a unique and separate password for your email.
- Use three random words to create a strong and memorable password.
- Store your passwords somewhere safe: save to your browser or use a password manager.
- Add extra security to important online accounts: turn on two-factor authentication.

Look after your devices…

- Set your phone and tablet to automatically update.
- Install the latest updates on your phone and tablet when prompted.
- Turn on back up for data stored on your phone and tablet.

Learn more about how you can stay safe online

https://www.ncsc.gov.uk/section/information-for/individuals-families

NCSC Annual Review 2019

BE CYBER SAVVY!

October is Cyber Security Awareness Month!
The following best practices will help ensure you are practicing good cyber security at home and at work!

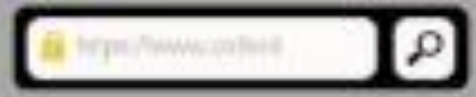
MULTIPLE PROFILES

Use different usernames and passwords for:

- Social networking sites
- Finance sites (banks)
- Shopping sites
- Work

ONLY VISIT SECURE SITES

For online transactions using username and password, make sure that the site is secure. Sites that are secure will have a https:// website address.



Secure sites are also less vulnerable to compromise.

STRONG PASSWORDS

Create strong passwords by using passphrases for passwords and different characters for letters.

MyDOgW@Sph
@anIwrs@ry1991!

PROACTIVE SECURITY

If you hear on the news of a breach of a site you visit, immediately change your password - even if they are telling you that you are not affected!

SECURE YOUR DEVICES

Install and maintain an anti-virus program on your devices - including your mobile phone!

Don't forget to reboot after your security and virus program updates.

BE SUSPICIOUS

Immediately delete suspicious emails, and do not click on ANY links you cannot confirm are real!

A foreign prince isn't really going to split $1,000,000 with you.

BEWARE OF PHISHING

Phishing is a form of cyber crime that uses email and other communication mechanisms to trick people into divulging personally identifiable information, or PII.

PII is data that can be used to identify a specific individual - such as a social security number.

MONITOR YOUR ACCOUNTS

Always monitor your accounts for suspicious activity and immediately report anything suspicious.

- *Bank Accounts*
- *Credit Cards*
- *Commerce Sites*

STAY OFF PUBLIC WIFI

Connecting to public WiFi at an airport, hotel, or public space is opening you up to possible threats.
Do your best to avoid connecting your devices unless absolutely necessary.

OXFORD

Sources of info

- NCSC
  - blogs
  - Training - https://www.ncsc.gov.uk/static-assets/training/top-tips-for-staff-web/story_html5.html
- Cyber Essentials
- ICAEW – icaew.com/cyber

A final word.....