BARCLAYS

Digital Safety, Fraud & Scams

January 2020

Digital Eagles

Agenda

- An insight into Cybercrime, Fraud and Scams
- Tactics used by fraudsters
- Common Scams
- Top tips and best practice
- Useful Resources

Facts and Figures

Cybercrime [1]

is the 2nd biggest threat to the UK behind terrorism

You [2]

are more likely to be a victim of fraud or cybercrime than any other offence

£1.2 billion [3]

successfully stolen through fraud and scams in 2018

Identity fraud [4]

reached a record level in the UK, rising fastest for victims over 60 and under 21

1. CPNI | Centre for the Protection of National Infrastructure | National Security Threats
2. ONS | The Office for National Statistics | Crime Survey for England and Wales year ending March 2018
3. Cifas Fraudscape 2019 report
4. Cifas Fraudscape 2019 report

What is Cybercrime?

‘Criminal activities carried out by means of computers or the Internet’

Cybercrime involves any criminal act conducted through computers, networks and the Internet.

Why is it so successful?

- Technology
- Simple
- Cheap
- Anonymous
- High reward

Psychology behind fraud & scams

Watch out for emotions

Greed Urgency Curiosity Fear

Remember most fraudsters want you to do something.

They want you to use the faster thinking part of your brain used to make snap decisions without thinking as this significantly increases their chances of success.

What's your digital footprint?

- Name and Date of Birth
- Full address
- Family
- Photos
- Personal and Work Email Address
- Employer and Job Role
- What You Look Like
- Interests and Hobbies
- Recent Activity
- Current location

Social Engineering

> The clever manipulation of the natural human tendency to trust

Tony Blake
Dedicated Card & Payment Crime Unit

Fraudster's tactics

Phishing

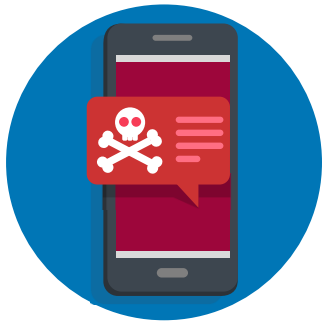
Spoof **emails** trying to get the recipient to:

- Click on a link
- Open an attachment
- Give away information
- Make a payment

Vishing

Spoof **phone** call trying to get the recipient to:

- Divulge security details
- Pay or transfer money
- Give away information



Smishing

Spoof **text message** trying to get the recipient to:

- Click on link
- Pay money
- Give away information
- Call premium number

Ransomware and fake websites

Common Scams

Safe Account Scam

HMRC Tax Scam

Romance Scam

Investment Scam

Holiday Scams

Ticket Scams

Identity Fraud

Fraudsters steal enough bits of personal information about you in order to impersonate you. They then take out loans and credit cards in your name, or withdraw cash from your bank account.

How to prevent Identity Fraud:

- **Check your bank accounts** regularly for any unusual items or spending, anything you don't recognise – report it to your bank.
- **Keep a close eye on your credit rating** and watch out for any unexpected activity on it.
- **Be suspicious about any phone call, texts, emails or social posts** claiming to be your bank, an organisation or other company and which ask for personal info.

Money Mules

> In 2018, organisations reported over 40,000 cases of fraudulent abuse of bank accounts that
> bore the hallmarks of money mule activity.

Cifas Fraudscape report 2019

A money mule is an individual who allows his/her bank account to be used to move criminal funds in return for easy money or goods.

This is a form of money laundering and if you knowingly allow your account details to used for fraud you could face a prison sentence.

How secure is your password?

Top 10 Passwords

1. 123456
2. password
3. 123456789
4. 12345678
5. 12345
6. 111111
7. 1234567
8. sunshine
9. qwerty
10. iloveyou

Did you know?

Due to cyber attacks and data breaches, criminals have access to millions of passwords!

Source: SplashData's Top 100 Worst Passwords of 2018

Passwords – top tips

- Review all your passwords.
- Create a strong separate password for each account.
- Use three random words to create a strong password, you could add numbers and symbols too.

For example: 3redhousemonkeys27!

Remember!

Your password is the key to your personal and financial information

- Never use personal details in your password such as your child's name or favourite sports team which could be easy for people to guess.
- Consider using a trusted password manager to store your passwords.

Two-factor authentication

Two-factor authentication (2FA) provides a way of 'double checking' that you really **are** the person you are claiming to be when you're using online services, such as banking, email or social media.

It is available on most of the major online services. Go to the settings option to turn on and activate this security feature.

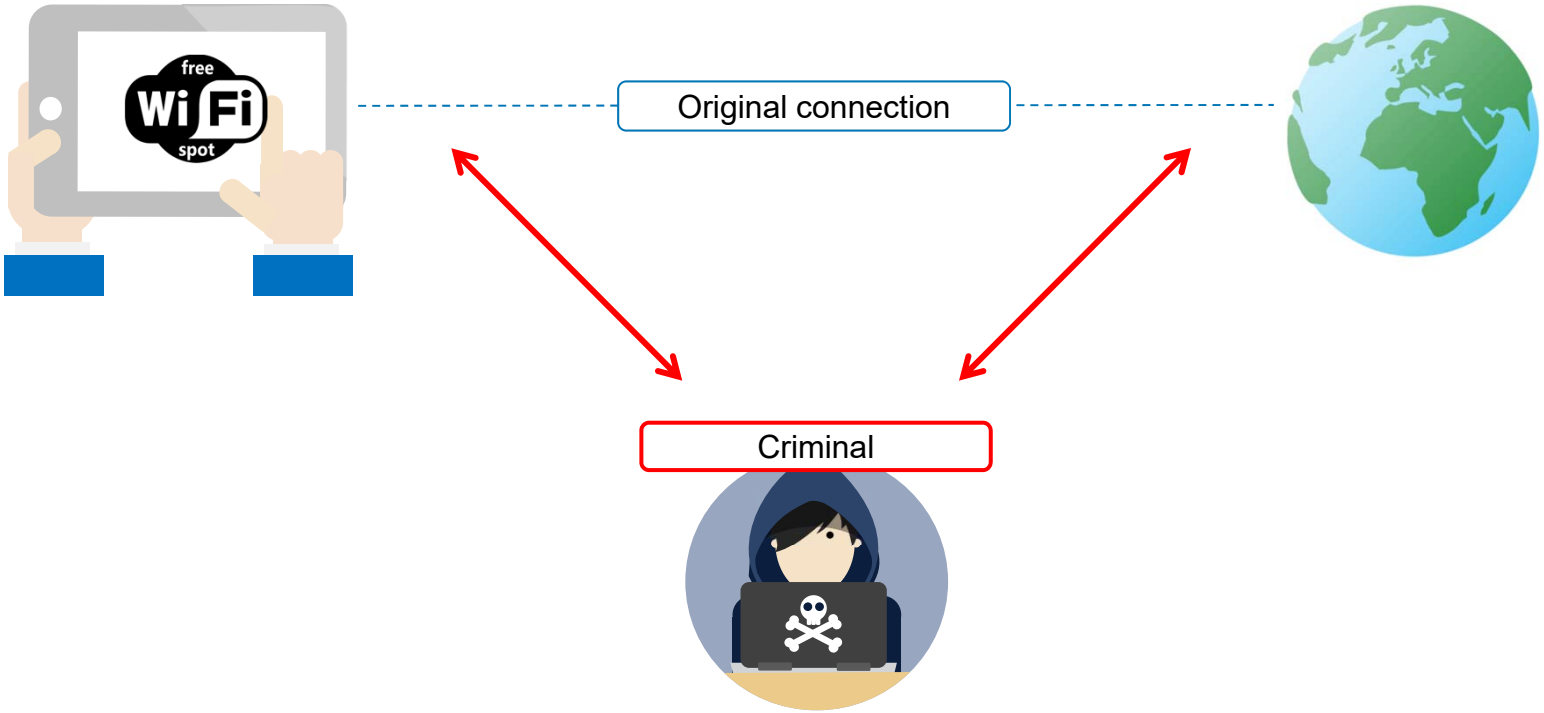
A common way 2FA works is by sending a one use only verification code to your phone which you will need to enter along with your username and password to access your accounts.

2FA

An extra layer of security is a great way to ensure it's only you who is accessing your information

586240

Using Public Wi Fi – know the risks



Key ways to protect yourself

- Use strong passwords and use two-factor authentication.
- Never share your bank PINs, passcodes or login details.
- Make sure that all your security software is up to date.
- Don’t automatically trust any link, attachment, text message, phone number or email.
- Review your social media privacy settings and think twice before you post.
- Always back up your most important data.
- Remember if a deal or offer sounds too good to be true then it probably is.

STOP, THINK, ACT

Useful Resources

https://www.barclays.co.uk/digisafe/

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

https://www.getsafeonline.org/

https://takefive-stopfraud.org.uk/

https://www.friendsagainstscams.org.uk/

https://www.victimsupport.org.uk/