STAFFORDSHIRE POLICE

Cyber Champion Tips – May 2021

Two Factor Authentication

Last month we looked at the importance of strong passwords and discussed how to create one, but having a strong password is not enough to keep you safe in the online world, what happens if your password is stolen or compromised, is one security step enough?

strong password = 🔒 **one security step, is it enough ?**

Two factor authentication (2FA) is an important step to help keep you safer and adds another layer of security to online accounts and digital devices. 2FA supports a multi-layered approach to cyber security and can help reduce the risk of accounts being accessed by cyber criminals.

So, what is it and how does it work?

Two Factor authentication is a way of combining security factors together, making it harder for unauthorised people gain access, for example, in the event your password is stolen, a second factor/or step, would be needed to get into that account. It is a 'two step' process and also helps to prove 'you are who you say you are' to online providers. In physical security, it is like having two security features on a door instead of one to make it stronger, in cyber security, it works like this:

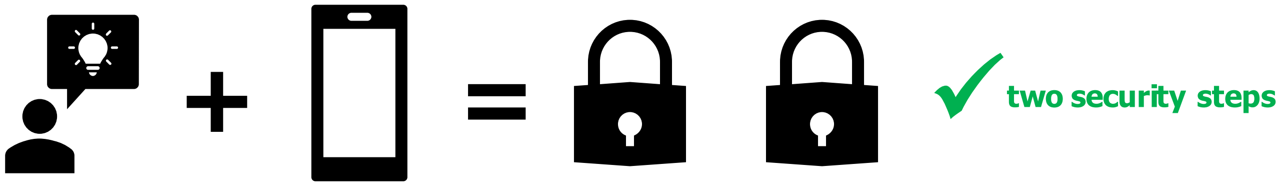
We apply **a combination of two** of the following:

1. **Something you know** - for example a strong password
2. **Something you are** - for example a biometric, such as your fingerprint
3. **Something you have** - for example a code to a mobile device, commonly via text or authenticator app

For example, 'something you know and are':

+ = 🔒 🔒 ✓ **two security steps**

Or, 'something you know and have':



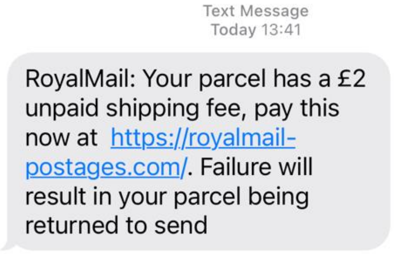
Setting up 2FA and using a combination of two or more of these steps, will really help to support better cyber security and help keep your online accounts and devices safer.

You can set up 2FA for most online accounts and devices and it is advisable to do so where possible; for further guidance on how to do this visit the National Cyber Security Centers (NCSC) website here: https://www.ncsc.gov.uk/guidance/setting-two-factor-authentication-2fa

Fake Text Messages - Smishing'

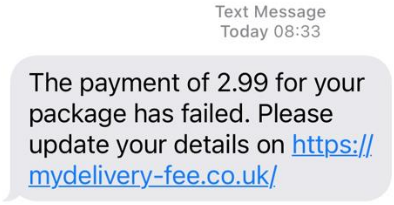
We must continue to be vigilant of fake text messages, also known as 'Smishing'. There has been a significant rise seen in the last couple of months of texts purporting to be from banks and delivery companies. Fraudulent text messages typically contain a link, which if clicked will take a person to a website which looks quite genuine, but it won't be. The purpose of these messages is to capture personal and financial details in order to scam an individual for money and/or conduct other fraudulent activity against a person.

Below are examples of fraudulent texts seen circulating recently, if you read the content of those shown, you will see that each one is **asking the recipient to do something** - 'update details' 'pay this now', 'if this was NOT done by you, visit', they are all designed to get a response:



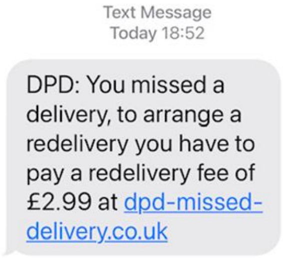
Text Message
Today 13:41

RoyalMail: Your parcel has a £2 unpaid shipping fee, pay this now at https://royalmail-postages.com/. Failure will result in your parcel being returned to send



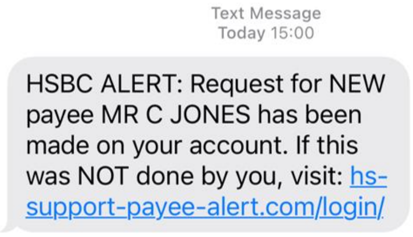
Text Message
Today 08:33

The payment of 2.99 for your package has failed. Please update your details on https://mydelivery-fee.co.uk/



Text Message
Today 18:52

DPD: You missed a delivery, to arrange a redelivery you have to pay a redelivery fee of £2.99 at dpd-missed-delivery.co.uk



Text Message
Today 15:00

HSBC ALERT: Request for NEW payee MR C JONES has been made on your account. If this was NOT done by you, visit: hs-support-payee-alert.com/login/

It always pays to **'Take Five'** if you are in receipt of a text message like this, ask yourself what is being asked 'of' or 'from' you. Always check a request using a safe sorce, contact the organisation directly and never resond to messages like these.

TAKE FIVE - STOP CHALLENGE PROTECT

Report suspicious texts by forwarding to **7726**

NEWS

Eight men have been arrested in dawn raids targeting scam text messages - Whilst on the subject of fraudulent text messages, there has been some positive news with BBC News reporting 'eight men have been arrested in dawn raids targeting scam text messages, the suspects were allegedly involved in sending fake messages, primarily posing as Royal Mail and asking people to pay a fee to retrieve a parcel' *BBC News*. The full BBC article can be seen here: https://www.bbc.co.uk/news/uk-england-57226704

Investment Scams - Action Fraud state 'New figures reveal victims lost over £63m to investment fraud scams on social media'

Action Fraud have seen a significant increase in the rise of investment scams. It seems that social media platforms are playing a factor in investment scams and more under 30's are becoming affected by scams in this way. Social platforms offer more opportunity for criminals to target individuals; by contrast, where social media wasn’t a factor, the average age of people being affected is over 50.

'Fraudsters present professional and credible looking online adverts, send emails, and create websites to advertise fake investment opportunities in cryptocurrency, foreign exchange trading and bonds. Often, fake testimonials are accompanied with a picture of a well-known figure to help the investment seem legitimate. Between April 2020 and March 2021, Action Fraud received over 500 investment fraud reports which made reference to a bogus celebrity endorsement, with losses reaching over £10m.

How can you protect yourself?

- Be suspicious if you are contacted out the blue about an investment opportunity. This could be via a cold-call, an e-mail or an approach on social media.
- Don’t be rushed into making an investment. No legitimate organisation will pressure you into making a transaction, or committing to something on the spot. Take time to do your research.
- Seek advice from trusted friends, family members or independent professional advice services before making a significant financial decision. Even genuine investment schemes can be high risk.
- Use a financial advisor accredited by the Financial Conduct Authority (FCA). Paying for professional advice may seem like an unnecessary expense, but it will help prevent you from being scammed.
- Always check the FCA Register to make sure you’re dealing with an authorised firm and check the FCA Warning List of firms to avoid.
- Only use the telephone number and email address on the FCA Register, not the contact details the firm gives you and look out for subtle differences.
- Just because a company has a glossy website and glowing reviews from ‘high net worth’ investors does not mean it is genuine – fraudsters will go to great lengths to convince you they are not a scam.
- Remember, if something sounds too good to be true, it probably is.

If you think you’ve been a victim of an investment fraud, report it to Action Fraud online at www.actionfraud.police.uk or by calling 0300 123 2040. For more information about investment fraud, visit www.fca.org.uk/scamsmart.' *Action Fraud*

Good News

Phishing - Suspicious Email Reporting Service (SERS) Update:

Hopefully, everyone is getting into the habit of forwarding suspicious emails they receive to SERS. The combined efforts of the public reporting and action undertaken by the service, has seen some excellent work done, with latest figures showing:

'As of 30th April, the number of reports received stand at more than 5,800,000 with the removal of more than 43,000 scams and 84,000 URLs.

Thank you for your continued support.' *NCSC*

This is fantastic work and means that every for removal of a scam or malicious URL, less people will be affected by this type of criminality. So, if you are not quite sure about an email you've received, forward it to the Suspicious Email Reporting Service (SERS):

report@phishing.gov.uk

NCSC NEWS

New eLearning for small organisations and charities:

Free eLearning for small organisations and charities is now available from the NCSC. 'Most small organisations do not have an IT department, or technical staff responsible for cyber security and with so much cyber security advice out there, it can be difficult for small organisations to know where to start' *NCSC*. The training is easily accessible to all staff and covers five key areas of learning, to learn more and access the training visit here: https://www.ncsc.gov.uk/blog-post/training-for-small-organisations-and-charities-now-available

New 'Early Warning Service' for medium to large organisations:

The new Early Warning Service from the NCSC, is designed to help organisations defend against cyber-attacks by providing timely notifications about possible incidents and security issues. The free service automatically filters through trusted threat intelligence sources to offer specialised alerts for organisations so they can investigate malicious activity and take the necessary steps to protect themselves. The service uses a variety of information feeds from the NCSC, trusted public, commercial and closed sources, which includes several privileged feeds which are not available elsewhere. Find out more about this new service here: https://www.ncsc.gov.uk/information/early-warning-service

May NCSC threat reports here:

7th May 2021 - https://www.ncsc.gov.uk/report/weekly-threat-report-7th-may-2021

- Hoax COVID-19 vaccine website taken down
- Multiple Vulnerabilities Affecting the Exim Mail Server
- Updated advice on Pulse Connect Secure RCE Vulnerability
- Ransomware Task Force publishes framework to tackle ransomware threat

- Further TTPs associated with SVR cyber actors
- Reporting to the NCSC

14th May 2021 - https://www.ncsc.gov.uk/report/weekly-threat-report-14th-may-2021

- Colonial Pipeline hackers didn't intend to cause problems
- Microsoft May 2021 security updates
- Over 25,000 servers in the UK still running vulnerable Exim versions
- Active Cyber Defence takes down 1.5 million malicious cyber scams

21st May 2021 - https://www.ncsc.gov.uk/report/weekly-threat-report-21st-may-2021

- Survey launched to help improve diversity in the cyber security industry
- Leaky AWS S3 bucket 'leaves job hunters' data exposed'
- Prison sentence for COVID-19 vaccine SMS scammer

West Midlands Regional Cyber Crime Unit (WMRCCU):

The WMRCCU website has a host of information to help boost your cyber awareness and help keep you informed, take a visit where you will find tips, information, advice, podcasts and subscription to the Cyber Crime Sentinel, check it out here: https://www.wmcyber.org/

Reporting

Report cyber-crime and fraud to Action Fraud: actionfraud.police.uk

Businesses suffering a live cyber-attack can call: 0300 123 2040

ActionFraud
National Fraud & Cyber Crime Reporting Centre
0300 123 2040

Received a phishing email?

Forward suspicious emails to: report@phishing.gov.uk

Received a suspicious text message?

You can report fraudulent texts by forwarding to: **7726**

If a scam text claims to be from your bank, you should also report it to them

Further advice can be found by visiting:

cyberaware.gov.uk

ncsc.gov.uk

actionfraud.police.uk

takefive-stopfraud.org.uk

ukfinance.org.uk

staffordshire.police.uk

TAKE FIVE TO STOP FRAUD