September Cyber Scam Update

Parcel delivery texts now the most common con-trick

Millions of mobile users have received the texts that claim a small payment is needed for a package delivery to be completed. But the texts are a front for fraudsters attempting to steal personal banking details. Cybersecurity firm Proofpoint told banks their prevalence was on the rise.

Impersonation

Smishing is a technique that criminals use to target consumers with texts impersonating trusted organisations.

Proofpoint, which provided data for the banking trade body UK Finance, said that over a 90-day period to mid-July, some 53% of these smishing attempts were via delivery texts. This compared with 23% of messages claiming to be from banks or financial institutions. During the most recent 30-day period, some 67% of these scams were delivery text messages.

Tricked in a hurry

The text, claiming to be from Royal Mail or a delivery company arrives out of the blue and claims a parcel is awaiting delivery, but a small payment is required.

The message then links to a website mocked up to look like an official site. The page requests personal and payment details, which scammers may use to steal someone's identity, or use to target them with other scams.

Royal Mail said it would not use such texts - unless specifically requested - and would use a grey card instead to tell people if any fee was required.

- To report scams, contact Action Fraud
- To report email scams, contact the National Cyber Security Centre (NCSC) by emailing report@phishing.gov.uk
- For consumer advice, please call the Citizens Advice Consumer Helpline on 0808 223 1133

If you fall victim to any scam, report to Action Fraud on 0300 123 2040 or http://www.actionfraud.police.uk

If you would like support as a result of becoming a victim of any crime, contact Victim Support on 01926 682 693.

40 million T-Mobile customers hit by US data breach

The breach was blamed on a "highly sophisticated cyberattack". It said it is "taking immediate steps to help protect all of the individuals who may be at risk from this cyberattack". The firm said that while criminals stole personal information, no financial details were leaked as a result.

The breach only came to light following online reports last weekend that criminals were attempting to sell a large database containing T-Mobile customer data online. The US telecom giant confirmed that hackers had gained access to its systems on Monday.

The company said its investigations identified approximately 7.8 million current T-Mobile post-paid customer accounts' information in the stolen files, as well as just over 40 million records of former or prospective customers who had previously applied for credit with T-Mobile. It said that approximately 850,000 active T-Mobile prepaid customer names, phone numbers and account PINs were also exposed but that it had reset all of the PINs on the accounts to protect customers.

It added that no phone numbers, account numbers, PINs, passwords, or financial information were compromised in any of the files of customers or prospective customers. Hackers previously stole the personal information of 15 million T-Mobile customers and potential customers in the US in 2015. There is no indication yet that former UK customers of T-Mobile have been hit by the data breach.The company's UK operation T-Mobile UK was rebranded as EE in 2012 and sold to BT in 2016 for more than £12bn.

September Cyber Scam Update

Vaccine Passport Scams

The emails claim to be able to provide people with a "digital passport" that "proves you have been vaccinated against COVID-19". These emails are fake, and the links within them lead to genuine-looking websites that steal your personal and financial information.

How to protect yourself:

In the UK, coronavirus vaccines will only be available via the National Health Services of England, Northern Ireland, Wales and Scotland. You can be contacted by the NHS, your employer, a GP surgery or pharmacy local to you, to receive your vaccine. Remember, the vaccine is free of charge. At no point will you be asked to pay.

- The NHS will never ask you for your bank account or card details.
- The NHS will never ask you for your PIN or banking passwords.
- The NHS will never arrive unannounced at your home to administer the vaccine.
- The NHS will never ask you to prove your identity by sending copies of personal documents such as your passport, driving licence, bills or pay slips.

Your vaccination status can be obtained for free through the official NHS app, NHS website, or by calling the NHS on 119.

How to report scams:

If you receive a call you believe to be fraudulent, hang up. If you are suspicious about an email you have received, you can report it by forwarding the email to: report@phishing.gov.uk. Suspicious text messages can also be reported by forwarding them to the number: 7726 (it's free of charge).

If you believe you are the victim of a fraud, please report this to Action Fraud as soon as possible by calling 0300 123 2040 or visiting www.actionfraud.police.uk.

MONTHS TOP TIPS:

Protect yourself from Viruses and Malware:

- Make sure your computer has a firewall and reputable anti-virus software. Without these, your computer has no defence to block infections.
- Take care downloading files. If you don't know someone who's sent you an email with an attachment, or you're not sure about a website offering a file to download, don't do it out of curiosity.
- Browse safely on the web. Get to know the risks and use the same level of caution as you would in the real world.

Keep up to date with the latest updates on Community Safety in Warwickshire.

Like us on **Facebook**: www.facebook.com/SafeinWarwickshire

Follow us on **Twitter**: @SafeInWarks

Visit our **site**: www.safeinwarwickshire.com

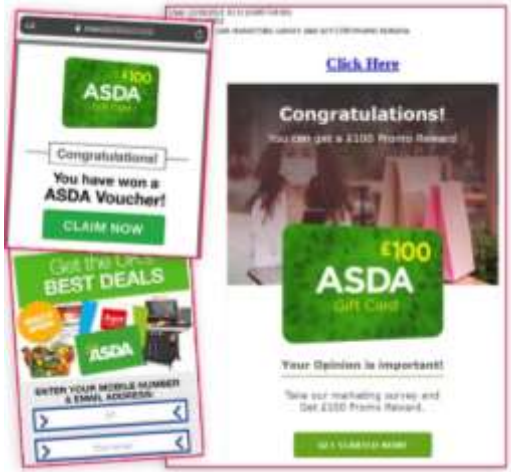
3 2040 or http://www.actionfraud.police.uk

crime, contact Victim Support on 01926 682 693.

Watch out for this Asda gift card scam!

Action Fraud have received 159 reports within 48 hours about fake emails purporting to be from Asda.

The emails state that the recipient can win a "£100 promo reward gift card" by completing a marketing survey. The links provided in the emails lead to phishing websites that are designed to steal your personal information.



TOP TIPS:

Your bank, or any other official organisation, won't ask you to share personal information over email or text. If you need to check it's a genuine message, call them directly.

Spotted a suspicious email? Forward it to the Suspicious Email Reporting Service (SERS) – **report@phishing.gov.uk**