safe in...
warwickshire

January Cyber Scam Update

CYBER
SAFE
WARWICKSHIRE

Fake DPD messages lead to over £200,000 in losses since June

The Suspicious Email Reporting Service (SERS), a tool launched by the National Cyber Security Centre (NCSC) and the City of London Police earlier this year, received thousands of reports of suspicious DPD emails.

The messages purporting to be from DPD claims that the delivery driver was "unable to deliver your parcel today" as "you weren't in or there was no safe place to leave it". The message provides instructions on how arrange another delivery. The links in the messages lead to fraudulent websites that request a small payment to rearrange the delivery.

If the victim makes this payment, they'll receive a phone call within a few days from someone purporting to be from their bank to inform them about suspicious transactions on their account. Criminals carrying out this scam are able to use a tactic called 'spoofing' to make the call or text appear genuine by cloning the phone number, or sender ID, used by the bank.

The victim is informed that their bank account may be compromised and is instructed to transfer their money to what they believe is an alternative secure account to prevent further losses. In reality, their money is being transferred into an account under the criminal's control.

In other cases, suspects have gained enough personal details and security information during the phone call with the unsuspecting victim, to enable them to take out a loan in the victim's name. The criminals then transfer the loan to an account under their control.

dpd

Always remember:

- Your bank, or other official organisations, will never ask you to share personal or financial information over the phone, or via text or email. If you need to check that it's a genuine message, contact them directly.
- You can report suspicious emails you have received but not acted upon, by forwarding the original message to report@phishing.gov.uk.
- You can report suspicious texts you have received but not acted upon, by forwarding the original message to 7726, which spells SPAM on your keypad.
- For DPD, only emails sent from one of three DPD email addresses are genuine. These are dpd.co.uk, dpdlocal.co.uk or dpdgroup.co.uk.

Action Fraud warns of new courier fraud tactic

Victims have reported a particular tactic of being called by someone impersonating a police officer. The suspect uses the name Eric Shaw and gives over his badge number, in order to appear trustworthy to victims.

The suspect asks victims to move money to a "secure bank account" until the victims are sent a new national insurance number. In reality, their money is being transferred into an account under the criminal's control.

How to protect yourself and your loved ones:

- Your bank or the police will never call you to ask you to verify your personal details or PIN by phone or offer to pick up your bank card by courier. Hang up immediately if you receive a call like this.
- If you need to contact your bank back to check the call was legitimate, wait five minutes; fraudsters may stay on the line after you hang up. Alternatively, use a different line altogether to contact your bank.
- Your debit or credit card is yours: don't let a stranger take it from you. You should only ever have to hand it over at your bank. If it's cancelled or expired, you should destroy it yourself.

Spot the tell-tale signs:

- Someone claiming to be from your bank or local police force calls you to tell you about fraudulent activity, but is asking you for personal information, or even your PIN, to verify who you are.
- They're offering to call you back so you can be sure they're genuine, but when you try to return the call, there's no dial tone.
- They say they're trying to offer you peace of mind by having somebody pick up the card for you, to save you the trouble of having to go to your bank or local police station.

SCAM ALERT

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.

January Cyber Scam Update

Over £2 million lost to criminals impersonating well-known broadband providers

Action Fraud has received reports of criminals cold calling victims purporting to be calling from well-known broadband providers primarily, claiming that the victim has a problem with their computer, router or internet. The suspect persuades the victim to download and connect via a Remote Access Tool (RAT), allowing the suspect to gain access to the victim's computer or mobile phone. Some reports also state that criminals have been using browser pop-up windows to initiate contact with victims.

Victims are then persuaded to log into their online banking to receive a refund from the broadband provider as a form of compensation. This allows the suspect access to the victim's bank account, and the ability to move funds out of the victims account into a UK mule account.

Always remember:

- Genuine organisations would never contact you out of the blue to ask for personal or financial details, such as your PIN or full banking password.
- Never install any software, or grant remote access to your computer, because of a cold call.
- Don't contact companies promoting tech support services via browser pop-ups.
- Hang up on any callers that claim they can get your money back for you.
- If you have made a payment, contact your bank immediately. They can help you prevent any further losses.
- If you granted remote access to your computer, seek technical support to remove any unwanted software. If you need tech advice, look for reviews online first or ask friends for recommendations.

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

Malicious email campaign purporting to be Subway delivers Trickbot malware

Malicious emails purporting to be from sandwich company Subway UK are being reported by multiple sources, including consumers and security researchers alike. These malicious emails state that the recipient has completed an order and details of this are included within the communication. A link is contained within the email, which if clicked on leads to the download of a malicious Microsoft Office Excel (.xls) spreadsheet file containing the malware Trickbot.

Top Tips:

- When responding to emails or phone calls, never give your login or personal details. If you receive an email from a company that claims to be legitimate but is requesting these details, or a contact number tell them you will call them back. Use a contact number for the organisation that you have sourced reputably. Speak to them directly to confirm that the message is genuine
- If you detect a phishing email, mark the message as spam and delete it. This ensures that the message cannot reach your inbox in future.
- Never click on links or attachments in suspicious emails, and never respond to messages that ask for your personal or financial details.

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.