Priority: 5 4 3 2 1

CRIME PREVENTION

Get Safe Online Campaign January 2019 - Safe Payments

Get Safe Online will help you keep your online payments safe.

Trust Get Safe Online to help protect your finances with safer payments advice from the GSO experts

These days, you can pay for almost anything online: products, services, tickets, holidays … even your next car, van or motorcycle. You can donate to charity, buy a driving licence or passport or pay to download, stream, play or gamble. It's fast and convenient, but there are also risks attached, with cybercriminals doing all they can to divert your money into their pockets.

Please read Get Safe Online's expert tips for protecting yourself and your finances:

- **Don't pay for anything by transferring money directly to people or companies you don't know, however eager you are to buy.** If it's a fraud, it's doubtful the bank will be able to recover or refund your money. The safest way to pay for anything is by credit card.

- **Make sure shopping websites are authentic by carefully checking the address is spelled correctly.** Fraudsters can set up convincing websites with addresses spelled very similarly to the authentic one.

- **Ensure that payment pages are secure, by checking that addresses begin with 'https' ('s' is for secure) and there's a closed padlock in the address bar.**

- **When you've finished making an online payment, log out of your account.** Simply closing the page may not do this automatically.

- **Don't make online payments when using Wi-Fi hotspots, as these may be either not secure or fake, and your transaction could be intercepted.** Instead, use your data, a broadband dongle or VPN … or wait until you get home.

Other ways to keep your online payments safe:

- Fraudsters commonly advertise non-existent products, services, event tickets, travel, holidays, accommodation, gambling, gaming, used vehicles and much more. They use auction sites, social media, fake or copycat websites and even legitimate accommodation platforms. Don't pay any money – even a deposit – unless you have thoroughly researched the source and product/service concerned and found it to be authentic.

- If you receive an email, letter or phone call asking you to change payment details for a service, product or subscription, always call the company on the number you know to be correct, in case someone else is attempting to defraud you.

- Follow the simple tech basics of having up to date internet security software/apps loaded and running, and the latest updates to operating systems, software and apps. This could prevent getting infected by malware that diverts your online payments.

- Don't click on attachments in unexpected emails or links in random emails, posts or texts. Doing so could result in your online payments being intercepted.

- Accept any additional security measures offered by your bank, as they will help to keep transactions safe.

- Download mobile apps only from authorised app stores, otherwise they may be fraudulent.

- Use strong, separate passwords for your email accounts. These can be created by using three random words, with some characters replaced or added to with numbers and symbols.

For more information on how to make online payments safely, visitwww.getsafeonline.org/safepayments #safepayments

If you think you've been a victim of online fraud, report it to Action Fraud, the UK's national fraud and cybercrime reporting centre on 0300 123 20 40 or at www.actionfraud.police.uk. In Scotland, call Police Scotland on 101.

To contact Sussex Neighbourhood Watch please E-mail enquiries@sussexnwfed.org.uk or visit www.sussexnwfed.org.uk.

Message Sent By
Derek Pratt (NHWN, Administrator, Sussex)