Online Safety Campaign

#PoliceScotlandKeepsafepostfestivescams

Police Scotland is reminding our communities to be on guard against scammers.

The period following the festivities can be a busy time for many people and criminals take advantage of this seeking out opportunities to commit frauds both online and offline.

Frauds can be committed by letter, texts and calls, but as more people shop, bank and do business online, criminals are now looking for more online opportunities to SCAM and gain access to people accounts, direct people to fake websites or have money sent to fraudulent accounts.

Criminals are often highly convincing and it is important to be aware of the warning signs - anybody or thing connected to the internet is a potential victim.

Sergeant Steven Gillies, who is part of the Safer Communities team within Police Scotland's Specialist Crime Division, has answered a number of key questions and has good advice to offer about how to stay safe online.

What are Scams?

Scams are fraudulent schemes that coerce people into parting with their personal or banking details and/or cash. Here are some popular types of scams:

- Phishing – A website, email or message that poses as a brand or company you recognise, usually the intention of this is to cause the recipient to click on a link or button within the message.
- Online Shopping & Auction Fraud – websites and auction listings where items that don't exist or are of inferior quality are listed for sale. Often fake websites are set up to trap people into making purchases with great deals and low prices.
- Vouchers – scammers often convince people to pay for fake services by purchasing popular music vouchers and sending on the code.
- Vishing – similar to phishing, this time conducted over the phone, the recipient is coerced into handing over personal information, banking details or passwords.
- Lottery/big money wins – unsolicited letters are sent advising of a large lottery win or money due following a death. To release this money you need to send cash to the fraudsters.

POLICE SCOTLAND
Keeping people safe
POILEAS ALBA

How to protect against Scams

- Don't assume anyone who's sent you an email or text message or has phoned you is who they say they are. It's imperative that you know the origin of those who contact you. If you feel unhappy about the content, delete the email or message or hang up the phone.
- Be sure to check the site you are visiting is secure, this is usually indicated by HTTPS in your browser bar address and often accompanied by a small padlock symbol. This usually means the information you send is secure.
- Buy from reputable and trusted companies that you know to be legitimate and genuine. Be very wary of sites offering 'too good to be true' deals
- Don't access your bank or building society accounts via email/message links received, go directly to the website
- Remember, a bank will never call or email and ask you for passwords, account details or to move money to a 'safe account'. Always double check numbers you're given to call back on or call through the main customer service number for the organisation. If you're still unsure, consider visiting your local branch instead of speaking to someone over the phone.
- Reputable companies will never ask you to pay for goods with vouchers or music tokens and never make large purchase with vouchers to pay for goods online.
- Never respond to letters or emails claiming that you have won or you are due money and never send any money to emails claiming they will release apparent winnings to you.

@PoliceScotland

PoliceScotland

scotland.police.uk

How do I know if I've been scammed?

- You may have difficulty accessing your online bank account or there may be unusual activity on your statements.
- Your computer may start to run slow, you may start getting an unusually high number of unsolicited messages.
- Bank or credit card statements usually sent to your address aren't delivered - this could be a sign of ID fraud.
- You have trouble obtaining credit when you've got a good credit history.

Can I get my money back?

Once money has been sent it can be incredibly difficult to get funds back if you don't use a trusted payment method. Ensure you use methods such as credit/debit cards, PayPal, Apple pay and Google Wallet for example, when making online payments as they have fraud protection measures in place.

If asked, never send cash or use carriers such as Moneygram or Western Union to forward on cash payments to unknown recipients.

What to do if you've been scammed

- Report the issue to Police Scotland on 101.
- Don't engage with the scammer, stop any interaction at once.
- Contact your bank, tell them and take advice.
- Contact the payment vendor and initiate resolution procedures.
- If possible keep all associated emails

Further preventative digital and cyber advice is available through the Police Scotland website at:

http://www.scotland.police.uk/keep-safe/keep-secure-online/ and from other prevention partners at the following sites:

Scottish Government Cyber Resilience

Scottish Business Resilience Centre

National Cyber Security Centre

2592-17 pm