Information sent on behalf of Neighbourhood Watch Scotland

Shopping On-line Make Sure You Stay Safe

Following a number enquiries for advice from Neighbourhood Watch members and Alert users about avoiding online shopping scams I have put together some straight forward advice. As the first section says 'Trust Your Gut' If it doesn't feel right it most likely isn't right.

Trust Your Gut
Just like you wouldn't go into a shop that you don't recognise and seems a little off to you, don't shop at stores online that give you a bad feeling and appear shady. If at any time during the shopping or checkout process you feel like the site is asking for too much personal information, just quit the transaction and leave the site. You may hate to leave behind a really good deal, but the money and time you could lose if someone gets your credit card information will definitely cancel out the benefits of a sale price. If the site looks like it was designed in the 90's, has a weird address, fills your screen with pop-ups, just forget about it.

Be Extra Careful If You Are Using A Mobile Device
Smartphones can basically do everything a computer can do nowadays, but that doesn't mean they are as protected against threats as your desktop. Most phones aren't equipped with the anti-virus software that you have on your computer, so it's easier for criminals to get malware on your mobile device that could help them steal information you enter. There's also the risk of your phone being stolen, so make sure it's password protected so any information you may have stored on it isn't easily accessed.

Don’t Use Public Wi-fi To Shop
Anytime you enter personal information using a public network, you're setting yourself up for identity theft. Most Wi-Fi hotspots don't encrypt your data, so any hacker can basically just pluck your identity out of the air if he has the right software. This applies to mobile phones, too, since you're often using nearby Wi-Fi. Be aware when you're using a hotspot that any information you send through the Internet could be picked up by strangers; if it's information that could make you vulnerable, wait until you get home to your protected network. It may be less convenient, but it's much safer.

Check Your Credit Card Statement Regularly
Using a credit card is really the only smart way to shop online. If you buy something from a scam site using a debit card, check, or cash, there's no way to get your money back. If you use a credit card, the card companies have to reimburse you for fraudulent charges. But they can't always catch purchases you didn't make or receive, so it's up to you to keep an eye on your statements. If you see something fishy on your statement, just contact your credit card company to dispute the charge and possibly get a new card so the charges won't continue.

Change Your Passwords Regularly
We know, we know. It's a pain to go through and change the passwords on all your online accounts, not to mention the trouble it'll take to try to remember them all. But if you really want to keep your information (and bank account) safe while

you're shopping via the Internet, it's essential to mix up your account passwords every three to six months. This puts the kibosh on any hackers who have managed to break into your account. You should also make sure that you don't have the same password across all your accounts, since that makes them all vulnerable if one is hacked.

Look For HTTPS On Link Rather Than HTTP
The Internet has a thousand different acronyms and it's impossible for those who aren't tech savvy to keep track of them all. One you really need to know if you're going to make online purchases, though, is HTTPS. The added "S" means that the way your information is being sent is secure. HTTPS using SSL, or Secure Sockets Layer, which encrypts the information flying through the wires so that only the intended recipient can see it. If you're considering buying from a site whose URL starts with HTTP, be careful with the information you share. Other signs of a secure site are a closed lock or unbroken key at the bottom of the screen.

Don’t Click On Email Links
Instead, type out the address in your browser to make sure you're going to the site you think you're visiting. Many phishing scams involve emails from what seem like legitimate sites — banks, online stores, anything you might trust — and then send you to a phoney site where they can gather your information to steal your identity. If you get an email from a site where you've shopped before, make sure you don't follow the links and don't provide any financial or personal information the email requests. Real sites won't ask for important information over email. If you have any doubts about an email's authenticity, go to the company's website and get in contact with them.

Update Your Browser
Each new version of your Internet browser, especially if you use one of the more popular browsers, gets a boost in security. Older browsers, besides not working as well with some websites, often have holes in their security that hackers have discovered and can exploit. The same goes for your operating system and anti-virus software. Updates will keep you ahead of would-be identity thieves and keep your credit safe.

Looking for advice call Consumer Advice Scotland 0800 316 1442. If you have been a victim of this type of crime call Police Scotland on 101.

Message sent by

Mark Armstrong (NHWN, Community Support Officer, NW Scotland)