Neighbourhood Watch Update

from West Mercia Police

Be Cyber Smart Campaign

Monday December 1st, 2014

On December 1, 2014, Warwickshire Police and West Mercia Police launched the #Be Cyber Smart campaign to raise awareness of internet-related crime and to give people the knowledge they need to protect themselves.

The first phase focuses on online shopping; urging people to carry out a few simple safety checks before parting with their hard-earned cash.

We have joined forces with Get Safe Online to encourage people to follow their '12 Online Safety Tips of Christmas'

The 12 Online Safety Tips Of Christmas – from Get Safe Online

1. Don't Transfer Money

Always pay for items you buy online by card on a secure payment page, by cheque or by cash, in person. However desperate you areto secure an item, never transfer money into the seller's account, as you may never see the goods or your money ever again.

2. Check that Payment Pages are Secure

Before you enter your card details on a payment page,make sure it is secure by checking that the address startswith 'https' (the 's' stands for 'secure')and there's a padlock or unbroken keysymbol in the browser window.

3. Use a Credit Card

Still talking about payments, remember thatyou have more chance of getting your moneyback in the event of problems if you pay

bycredit card rather than debit card. Somesellers may charge a premium, but it couldwell be worth the extra for your peace of mind.

4. Use Auction Sites Safely

At Christmas time, many of us buy from online auction sites. Always use trusted and well-known payment methods instead of paying sellers directly. Read the site and seller's conditions. And for your personalsafety if you're collecting in person, take someonewith you or let people know where you're going.

5. Check Out Bargains With Care

If you find or are emailed about an item that seems just too much of a bargain, itcould be a scam, fake goods or it doesn'tmatch the description. Remember, if itseems too good to be true, it probably is.

6. Use Social Networks Safely

Social networks are a popular medium for scams – and are becoming increasingly so. If you see a post promising something free of charge, free entry to a Christmas competition with a fantastic prize or perhaps an offer that seems just toogood to be true, consider very carefully before following it up.

7. Use Email Safely

An email urging you to click on a link to reveal a special offer, to open an attachment containing some great news, or to "confirm details" or "reset your account", could well be a scam, even if it appears to come from a reputable source. If in doubt, delete the email and don't respond to or forward it.

8. Look After That New Smartphone or Tablet

If you're buying or get bought a new smart phone or tablet, protect it by

downloading a reputable internet security App, and make sure it's safeguarded with a PIN. Install parental control software on kids' mobile devices, and chat to themabout how to use the internet safely.

9. Remember To Log Out

When you've finished your online shopping or bankingsession, always log out of the website or app… it only takes a second. Sometimes, just closing the windowdoesn't mean you've logged out, and someone else couldgain access to your account and personal details. Don'tforget to check and save purchase confirmation emails.

10. Make Sure Wi-fi Is Secure

At home or other premises you know, make sure the Wi-Fiis secured. When you're out and about – in the café, the pub or a hotel for example – you can't guarantee it's secured even if you have to enter a code. When you're shopping, banking or making other online payments, it's better to connect with 3G or 4G, even if it's slower.

11. Beware of Scam Phone Calls

If someone posing as a retailer calls you to confirm an online purchase, it could
well be a scam. The idea is that you won't remember the purchase, and call your
bank. However, the fraudster stays on the line, and tricks you into revealing your financial details. If this happens, hang up, don't call back, but report it to Action Fraud.

12. Check Bank Statements

Check your bank and credit card accounts regularly for irregular or unauthorised transactions. If you spot any entries you don't recognise, contact your bank without delay. Make sure your bank has your up-to-date contact details so they can alert you if they spot anything unusual.