Charlton Central Neighbourhood Watch (CCNW)

Supported by Charlton Central Residents Association (CCRA)

The 12 Scams of Christmas

'Tis the season for consumers to spend more time online - shopping for gifts, looking for great holiday deals on new digital gadgets, e-planning family get-togethers and of course, using online or mobile banking to make sure they can afford it all. But before logging on from a PC, Mac, or mobile device, please look follow these tips and avoid these scams to stay safe online.

Look for the Lock

Never ever, ever buy anything online using your credit card from a site that doesn't have SSL (secure sockets layer) encryption installed. You'll know if the site has SSL because the URL for the site will start with HTTPS:// (instead of just HTTP://). An icon of a locked padlock will appear, usually in the status bar at the bottom of your web browser, or right next to the URL in the address bar.

Use Familiar Websites

Start at a trusted site rather than shopping with a search engine. Search results can be rigged to lead you astray, especially when you drift past the first few pages of links. If you know the site, chances are it's less likely to be a rip off. We all know Amazon.com, and often other high street stores have an online store. Beware of mis-spellings or sites using .net instead of .com, as they may not be legitimate.

Don't Tell All

Be wary of how much personal information you give away at the online checkout – no retailer needs your date of birth to do business!

Don't wait for your Statement

Go online regularly to check your bank balance is as it should be, and query anything you are unsure of.

Use Strong Passwords

Create unique, strong passwords for any site you visit, and do not use the same password for all. If you do, and someone finds out what it is, just imagine what they could have access to!

Holiday Phishing Scams

Phishing is the act of tricking consumers into revealing information or performing actions they wouldn't normally do online using phony email or social media posts. A common holiday phishing scam is a **phony notice from UPS**, saying you have a package and need to fill out an attached form to get it delivered. The form may ask for personal or financial details that will go straight into the hands of the cyberscammer.

Think Mobile

If you are using your mobile to make online purchases, ensure you install the app provided directly by the retailer (like Amazon).

Avoid Public Terminals

If you do have to, then remember to fully log out every time, even if you were just checking emails. And if you are looking a laptop while out and about, sit with your back to the wall so no-one can snoop over your shoulder!

Gift Cards

Always make sure you buy these directly from the store, not from an auction website (eg eBay) as scammers often auction off gift cards with very little or no money left on them.

"I'm away from home" Scammers

Posting information about a holiday on social networking sites could actually be dangerous. If someone is connected with people they don't know on Facebook, they could see their post and decide that it may be a good time to rob them.

Holiday Screensavers

Bringing holiday cheer to your home or work PC sounds like a fun idea to get into the holiday spirit, but be careful. A recent search for a Santa screensaver that promises to let you "fly with Santa in 3D" is malicious. Holiday-themed ringtones and e-cards have been known to be malicious too.

Know What's Too Good to Be True

Remember – if it looks too good to be true, it probably is.

Have a safe and merry Christmas, from everyone at CC Neighbourhood Watch