**Safer Internet Day Tuesday 6th February, 2018**

**“Create, Connect and Share Respect: A better internet starts with you”**

The internet is one of the most amazing inventions of our time, offering us wonderful ways to communicate, find important information and tap into an endless supply of entertainment. That said, the web is also a place where you need to protect yourself from unscrupulous individuals.

Online, you need to watch out for the potential of both virtual and real threats, but there are a few easy ways to do so. Staying safe on the web means paying attention to the kind of personal information you share online, the type of sites you visit and the way you conduct yourself – find out how to browse safely and enjoy your time online.

With the vast increase in Internet use of the older generation or Silver Surfers comes the increased threat of becoming a victim of fraud type scams. This document highlights a few preventative measures and advice that could protect you from becoming a victim of this crime type

**Ways to improve your online security**

One of the most important things you can do when it comes to staying safe on the web is making sure that your passwords are unique and secure. Once someone can get into your password-protected information, they are able to find out all kinds of details about you and this puts you at a high risk of fraud. Google has some great [password advice](https://www.google.co.uk/intl/en/safetycenter/everyone/start/password/) for helping you make sure you have a good line of defence against cyber criminals.

There are five easy actions people can take in order to protect themselves and others from cyber-crime:

Using strong, memorable passwords

## Installing anti-virus software on new devices

## Checking privacy settings on social media

## Shopping safely online – always ensuring to check online retail sites are secure

## Downloading software and application patches when prompted

The most popular password is still ‘password’ making it easy for criminals to hack your accounts. The longest passwords of at least 10 characters are better. You could start with a line from the lyrics of a favourite song or a poem and then customise it in a way that’s relevant to you or your sense of humour.

**Tips for safe and secure online banking**



Banks take many measures to ensure that online banking is safe and secure. These include making sure their websites are encrypted, having timed log outs, deactivation of your login details if a number of incorrect attempts are made, and many authentication processes.

### **Top Ten tips for safe online banking**

* Keep your computer up-to-date with antivirus software.
* Be wary of unsolicited emails or phone calls asking you for PINs or passwords – your bank or the police would never ask for these in full.
* Always type your bank’s address into your web browser –  never follow a link in an email and then enter
* A locked padlock or unbroken key symbol should always appear in your browser window when banking online. The ‘http’ at the beginning of the website address will change to ‘https’ when a secure connection is made.
* When making a payment, always double check that you have entered the correct account number and sort code.
* Never leave your computer unattended when logged in and log off as soon as you’re finished, especially on any public computer.
* Check your statements regularly – if you notice anything strange, contact your bank immediately.
* Be wary of any unexpected or suspicious looking ‘pop-up’ windows that appear during your online banking session.
* Stop and think about the process you normally go through to make a payment to someone – be suspicious if it differs from the last time you used it.
* Fraudsters sometimes try to trick people into making a real payment by claiming “it’s just a test”.

## Watch out for scam emails

Phishing emails are sent by criminals posing as genuine companies such as a bank or HMRC. Clicking on a link takes you to a fake website where fraudsters steal financial or personal details.

Or, the link might install malware on your computer as another means to capture details. Thieves can steal your password by tricking you into installing a program on your computer that secretly records your password when you type.

**Seven ways to spot a Scam.** You may avoid falling for scams by asking yourself these seven simple questions. If you answer yes to any of the following, there's a good chance it's a scam.

## Contacted out of the blue?

An unsolicited call can be a sign of being contacted by a company you don't want to deal with. If you're called by a company, make sure you do all you can to verify the identity of the caller.

Ask them to give you details that only the company will know. For instance your service contract details, payment details or bank account details.  If you're not 100% convinced of the identity of the caller, hang up and contact the company directly from a different phone.

**Is the deal too good to be true?**

## Scams will often promise high returns for very little financial commitment. They may even say that a deal is too good to miss. Use your common sense, if a deal is too good to be true, it inevitably is.

## Asked to share personal details?

Never share your personal details with anyone you can't validate is who they say they are.

**Pressurised to respond quickly?**

Never proceed unless you are absolutely certain your money will be safe. Once you transfer, it may be too late.

Scammers will often try to hurry your decision making, always take a breath and think things through. Salesmen in particular should always give you time and space to make an informed decision, anyone who tries to rush you is not to be trusted.

## ****5**** Are the contact details vague?

Vague contact details can be a PO box, [premium rate number](https://www.which.co.uk/consumer-rights/advice/how-to-avoid-costly-calls) (starting ‘09’) or mobile number.

If anything goes wrong it's important you can contact those involved. This will be difficult if you don't have accurate contact information.

Premium rate numbers are also a favoured trick for squeezing every penny they can out of you.

## ****6**** Spelling or grammatical mistakes?

Legitimate organisations will rarely, if ever, make glaring spelling or grammatical mistakes, and if so they will usually be an isolated incident.

## ****7**** Are you asked to keep it quiet?

Being asked to keep something quiet should be a red flag. It's important you can discuss any agreements with your friends, family or independent advisors.

## Bank-transfer scams

Whereby fraudsters posing as your bank's fraud department convince you to move money from your legitimate account into a “new” account, because your current one has been compromised. Once the money has been transferred your money will be lost to you and your bank may not be liable to cover losses – because you authorised the payment.

[www.getsafeonline.org](http://www.getsafeonline.org)

[www.policescotland.co.uk](http://www.policescotland.co.uk)

Take five to stop fraud

**Online shopping fraud**

Shopping and auction fraud involves fraudulent shopping scams that rely on the anonymity of the internet.

As the popularity of internet shopping and online auctions grows, so the number of complaints about transactions is increasing. Some of the most common complaints involve:

-          buyers receiving goods late, or not at all

-          sellers not receiving payment

-          buyers receiving goods that are either less valuable than those advertised or significantly different from the original description

-          failure to disclose relevant information about a product or the terms of sale.

If you are a victim of shopping or auction fraud, the most immediate problem is that you have no real prospect of returning the goods or having your money refunded.

After this, there is a risk that your identity details could be compromised. Fraudsters could steal your identity and use it to access your personal finances or obtain goods or finance from alternative sources.

**Are you a victim of shopping and auction fraud?**

-          You’ve bought goods from an online seller that are either late in arriving or don’t arrive at all.

-          You’ve received goods from an online seller that don’t match the original description.

-          You’ve given identity details or personal financial information to an online seller who has used them in criminal ways.

**What should you do?**

-          If the seller has misrepresented the goods you’ve bought, report the fraud to Trading Standards

-          Keep all evidence of the offence, including goods and correspondence

-          If there is a business dispute over the nature of the transaction, contact the website involved. Or, you if you live in Stirling or Clackmannanshire Council areas contact Trading Standards on 01786 443322 or if you live in the Falkirk Council area contact Consumer Direct by phone on 08454 04 05 06.

**Protect yourself against shopping and auction fraud**

-          Make sure you understand how the website’s feedback function works. Feedback will give you useful information about recent transactions other buyers have made.

-          Check the item’s description carefully – ask the seller questions if you’re not sure of something.

-          Beware of people offering you a deal below the current bid or reserve price, especially if they contact you direct. Remember, if an offer sounds too good to be true, then it probably is.

-          Be extremely careful when buying things from people with little or no selling history.

-          Be aware of phishing emails that look like they come from the online auction or payment site you’re registered with, asking you to update your account details or re-enter them because your account has been suspended.

-          Check the URL in the web browser. A tactic often used by fraudsters is to change the address very slightly (if they’re spoofing an eBay site, for instance, they may have an address such as ‘. . . @ebayz.com’ whereas the real site is ‘. . . @ebay.com’)

-          Read the terms and conditions carefully, including those relating to any dispute resolution procedures the site offers.

-          If you bid for an item unsuccessfully, don’t be tempted to trade off-site if another seller approaches you with a similar item.

**As a buyer you should:**

 Try to avoid paying by money transfers – they aren’t secure.

-          Be careful when using direct banking transactions to pay for goods. Make sure transactions are secure.

-          Don’t send confidential personal or financial information by email.

-          Use an online payment option such as PayPal, which helps to protect you.

-          Check the URL in the web browser. A tactic often used by fraudsters is to change the address very slightly (if they’re spoofing an eBay site, for instance, they may have an address such as ‘. . . @ebayz.com’ whereas the real site is ‘. . . @ebay.com’)

-          Read the terms and conditions carefully, including those relating to any dispute resolution procedures the site offers.

-          If you bid for an item unsuccessfully, don’t be tempted to trade off-site if another seller approaches you with a similar item.