Scottish Business Resilience Centre

Creating a secure Scotland for business to flourish in

Is online security on your list this Black Friday?

Online security should be at the top of your list this festive season because your personal & financial information is always at the top of the list for cyber criminals.

The Norton Cyber Security Insights Report published today reveals that one in five Brits have been victims of cybercrime in the last year.

The good news is that there are a few simple steps you can take to ensure you are shopping safely online:

Checking the address bar

Https://

On any website where you are making a purchase or entering any personal information such as address or bank details always make sure that the information in the address bar at the top of the webpage begins with https://
The ‘s’ is essential as this indicates that there is a secure connection between your computer and the place where you are sending your personal details. Not all websites will have the ‘s’ as part of their url. It’s not necessary on websites where you are not providing any personal information but make sure any website that you do provide with your information has it.

Padlock Icon

The https:// is the most important indicator of a secure connection but some websites also provide a padlock icon in the address bar.

Green Address Bar

Some secure websites will also turn a portion of the address bar green to indicate that they are secure.

By taking the above into account you can safely do your Christmas shopping online.

Phishing Scams

You need to be careful about giving out your personal financial information over the Internet. Be suspicious of any e-mail with urgent requests for personal financial information because it's probably a scam.
Phishing is an attempt to criminally and fraudulently acquire sensitive information such as usernames, passwords and credit card details by masquerading as a trustworthy entity using e-mail e.g. receiving an e-mail purporting to be from your bank to update your details online by following a given link.

Avoiding this type of scam is reasonably easy if you can remember that:

- Scam e-mails are aimed to encourage the recipient to respond.
- Scam e-mails typically ask for personal information such as usernames, passwords, credit card numbers, social security numbers, etc.
- Scam e-mails are typically not personalised and some contain either bad spelling or bad grammar. Valid messages from your bank or e-

commerce company will be professional and correctly addressed with your name.

- Never click on any link to a bank, eBay, or other merchants. When in doubt, call the institution using the number listed in the phone book or on their legitimate website, not the one provided in the e-mail or link.
- Avoid filling out forms in e-mail messages that ask for personal financial information and never save them to your computer.
- Don't click on attachments.
- Run both anti-virus and anti-spyware applications. Firewall and privacy protection software are also a good idea. Update this software, as well as your operating system, on a regular basis.
- Use a cross-cut shredder or burn documents containing personal information.
- Do not store PINs on your computer or other mobile devices.
- Ensure that you're using a secure website when submitting credit card or other sensitive information via your Web browser.
- Check the beginning of the Web address in your browsers address bar - it should be "https://" rather than just "http://" and a padlock should appear in the lower right hand corner of the information bar.
- Regularly check your bank, credit and debit card statements to ensure that all transactions are legitimate.
- Order credit reports on yourself yearly and review them carefully.

Mobile Phones

Mobile phones often contain sensitive information about you so it makes sense to take some practical measures to keep your mobile phone safe.

Remember to:

- Keep your phone out of sight in your pocket or handbag when not in use
- Use your phone's security lock code, if it has one

- Record details of your electronic serial number (ESN) and consider separate insurance
- Property mark your phone with your postcode and door number to help police identify stolen ones
- Most phones have an IMEI (International Mobile Equipment Identity) number which is a unique identifier for the phone; you can obtain this number by typing *#06# (star hash 06 hash) into your mobile phone and it will display a 15 digit number
- Report a lost or stolen phone to the police immediately
- Inform your service provider if your phone is stolen or lost
- Register the serial numbers of your phone on www.immobilise.com

Try not to:

- Attract attention to your phone when you are carrying or using it in the street.
- Leave your phone in an unattended car - if you must, lock it out of sight. It only takes seconds for a thief to smash a window and steal your phone.

Online Safety Advice from Police Scotland

Think before you post photos of your Christmas night out online. What may seem funny in private could embarrass or humiliate someone in public. If in doubt, don't click! Remember, what goes online stays online!

When shopping online, make sure your web browser and internet security is up to date. Check the website payment page is secure and look for the padlock in the address bar before you enter any card details.

If you're buying your child a mobile or tablet for Christmas, think about how you can keep them safe online.

If you'll be away from home over Christmas or even just out and about, be careful about what you say on social networking sites – don't let thieves know your house will be empty.