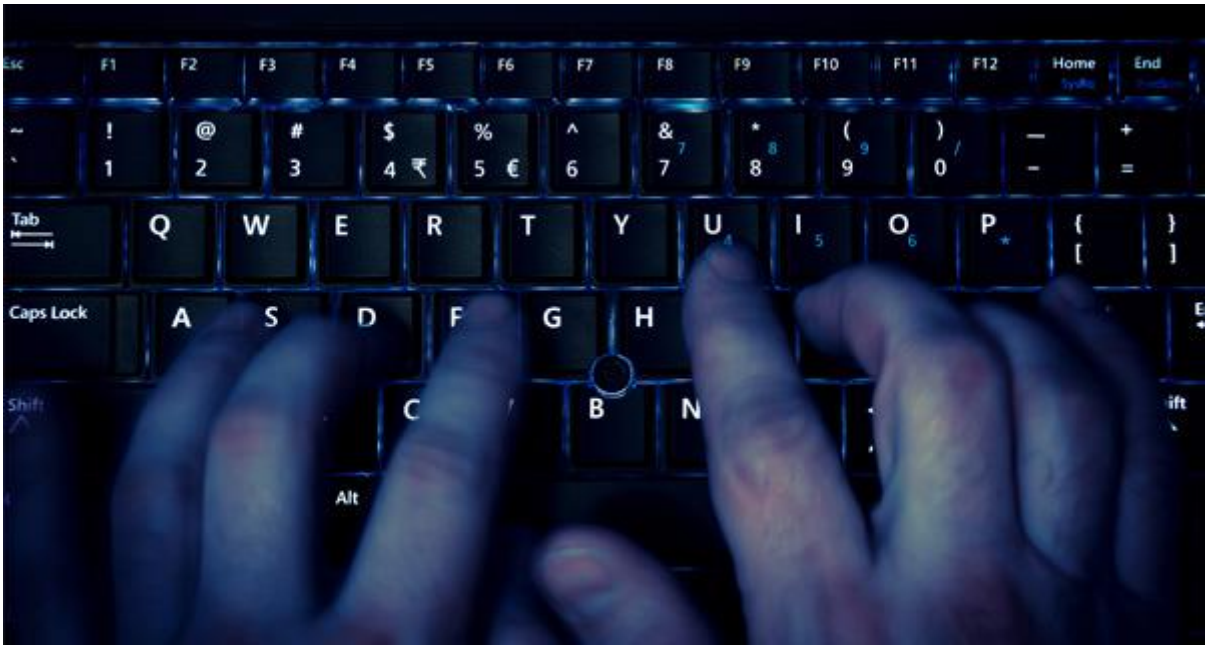
ALERTS

TRADING STANDARDS

16/12/2020

Protect yourself from fraud and cyber crime

Although fraud and cybercrime come in many forms, there are some simple steps you can take to protect yourself.



1. Do not give any personal information (name, address, bank details, email or phone number) to organisations or people before verifying their credentials.

Always question unsolicited calls, texts or emails requesting your personal or financial information (name, address, bank details, email or phone number). Instead, contact the company directly using a known email or phone number.

2. Make sure your computer has up-to-date anti-virus software and a firewall installed. Ensure your browser is set to the highest level of security and monitoring to prevent malware issues and computer crimes.

Always install the latest software and app updates on all your devices. Protect your email account with a strong, separate password and enable two-factor authentication (2FA) where possible.

Installing, or enabling, antivirus software on your laptops and computers will protect them from viruses and hackers.

3. Many frauds start with a phishing email. Remember that banks and financial institutions will not send you an email asking you to click on a link and confirm your bank details. Do not trust such emails, even if they look genuine. You can always call your bank using the phone number on a genuine piece of correspondence, website (typed directly into the address bar) or the phone book to check if you're not sure.

Never automatically click on a link in an unexpected email or text.

Remember, email addresses and phone numbers can be spoofed, so don't use those as a means to verify that a message or call is authentic.

The best way to get in touch with a company is to use a known email or phone number, such as the one on the back of your bank card.

4. Sign-up to Verified by Visa or MasterCard Secure Code whenever you are given the option while shopping online. This involves you registering a password with your card company and adds an additional layer of security to online transactions with signed-up retailers.

Layer up your protection. When shopping online, always check the web address to make sure you are on the correct site and sign-up to Verified by Visa or MasterCard Secure Code whenever you are given the option.

5. You should regularly get a copy of your credit file and check it for entries you don't recognise. Callcredit, Equifax and Experian can all provide your credit file. An identity protection service such as ProtectMyID monitors your Experian credit report and alerts you by email or SMS to potential fraudulent activity. If it's fraud, a dedicated caseworker will help you resolve everything.

You should regularly get a copy of your credit file. Callcredit, Equifax, Experian, ClearScore and Noddle can all provide you with a copy. If you spot anything suspicious, make sure your report it as soon as possible.

If you have been affected by a data breach that leaked your personal or financial details, monitor your credit file and bank accounts regularly for any unusual activity.

6. Destroy and preferably shred receipts with your card details on and post with your name and address on. Identity fraudsters don't need much information in order to be able to clone your identity.

7. If you receive bills, invoices or receipts for things that you haven't bought, or financial institutions you don't normally deal with or contact you about outstanding debts, take action. Your identity may have been stolen.

8. Be extremely wary of post, phone calls or emails offering your business deals out of the blue. If an offer seems too good to be true, it probably is. Always question it.

Listen to your instincts and be wary of unsolicited calls, emails or online ads offering deals that sound too good to be true.

Genuine banks, or other trusted organisations, won't pressure you into making a financial transaction, if something feels wrong then it's usually right to question it.

9. If you have been a victim of fraud, be aware of fraud recovery fraud. This is when fraudsters pretend to be a lawyer or a law enforcement officer and tell you they can help you recover the money you've already lost.

WHERE TO REPORT

Protect others by reporting incidents like this.

If you, or anyone you know, have been affected by fraud or any other scam, report it to Action Fraud by calling 0300 123 2040 or visiting www.actionfraud.police.uk

tradingstandards@royalgreenwich.gov.uk