Ten simple ways to stop online scammers

We are all becoming more vulnerable to financial fraudsters, but there are simple steps you can take to outwit them

Kenza Bryan

December 13 2019, 5:00pm, The Times

Patrick and Lais Haughian. Lias was hit by an online scam

Fraudsters are getting more sophisticated and scams are on the rise. With 3.9 million cases reported last year, you are much more likely to experience fraud than a violent crime.

Here are the best ways to avoid falling victim.

1. Choose a theme and stick to it

We all have to remember dozens of passwords these days so it is tempting to make them very simple. The best way to avoid accounts being hacked, though, is to choose long combinations of numbers, symbols and letters. To make them easier to remember, opt for a theme rather than just a memorable bit of information about you. For example, if you like Christmas, you could make it Chr*stm@$63. You can use favourite poems, songs or films. The options are endless.

2. Lie about personal information

When it comes to security questions for online accounts, you don't have to answer truthfully. Avoid giving your mother's maiden name because this is usually easy to find in electoral records or on your Facebook account. And unless you have shown remarkable restraint on social media, your pet's name is also likely to have ended up online, so don't use that either. Your answer can be anything. It could be cheesecake, or even toilet. Pick a random but memorable word, keep it secret and use it for every answer.

3. Set up extra security, but not by text
Passwords are a weak form of security, but you can add an extra layer by turning on two-step authentication for your online accounts. This means that you will receive a code that must then be produced to prove your identity when you make an online transaction. Try to avoid receiving the codes by text because they can be intercepted by fraudsters who convince your phone company to give them control of your number. We reported on the dangers of these Sim swap scams in last week's *Times* Money and security chiefs are warning banks against using text messages for authentication.

Facebook, Twitter and Google give you the choice of receiving the code in an authenticator application over the internet. Ask your bank if you can receive the codes in your mobile banking application (if you use one), or by card reader, email or phone call.

4. Hang up on strangers, even your bank
Fraudsters can use software that can make it seem as though they are calling or texting you from your bank's number. If your bank tries to call you, insist on calling back using the number on the back of your debit card and from a different phone line, if possible.

Be suspicious about calls from people you do not know, particularly if you are being asked for private information, bank details or any mobile-switching code that was texted to you from a phone company. Don't be afraid to hang up and call your bank to check whether it would ask you for these details. A legitimate company will understand.

5. Don't click on email links
Apply the same suspicion to any link sent to you by someone you do not know, whether by text or by email. If HM Revenue & Customs, Amazon, Apple, a parcel service or any other company suddenly emails when you are not expecting it, be suspicious and don't reply. Clicking on links can allow malicious software to be downloaded on to your phone or computer. They can also lead you to fraudulent websites that send your details to criminals. Check that the https at the start of the web address does contain the "s", which stands for secure and shows that the website is genuine.

6. Use a fine-tooth comb
Don't ignore bank statements. Scan them in detail for any strange payments. This is the best way of acting fast if you have fallen victim to fraud. Challenger banks such as Monzo will send you immediate notifications when you make a payment. If your bank does not offer this, print off your statement and highlight anything you do not recognise. If a payment description on your statement is an incomprehensible string of letters, type it into Google to find out which company uses this code.

7. Spy on your children
It sounds sneaky, but it is vital to keep a watchful eye on the social media accounts of your children. Ideally, only let your children use social media if they let you follow their profiles. This means that you can make sure they are not posting any personal information about the family online. Bank details are not the only risk; teach them not to post the dates on which you are going on holiday, pet names, or dates of birth of family members.

Also help them to understand the false lure of "easy money", a catchphrase often used in social media posts seeking to draw young people into money-laundering activities.

8. Get proof of delivery
If you are selling used items on eBay and send them by post, make sure you ask the courier for proof of delivery. It is more expensive, but otherwise the person receiving your item can claim that they never received it and will be able to dispute the transaction and get a refund from Paypal, the payment platform. If you hand over the goods in person and therefore can't get proof of delivery, ask to be paid in cash.

9. Be careful with payments
It has become so easy to send money online that we have all become a little blasé about it. Fraudsters prey on this. A common tactic is to hack into the emails of building contractors, plumbers or estate agents, supplying fake bank details. If you receive one of these emails, check directly with the company and be wary if it says that its payment details have suddenly changed.

Dating fraud is also on the rise, with 4,555 so-called romance scams reported to the official crime reporting organisation Action Fraud last year. Be wary of increasingly sophisticated deception techniques. For example, fraudsters can use footage of people they have never met to make you think that you are speaking to a real person in a video call online and to convince you they are in need of money.

10. Take five
If you only remember one thing, it should be that nothing is as urgent as it seems. Only criminals or stressed relatives will try to panic you into making payments or handing over information. Investments, shopping deals and online forms can wait five minutes. Take a deep breath and ring your bank or a friend to check that what you are being asked is legitimate.

I had weird texts, then my phone went dead and £4,000 vanished from my account
Mortgage broker Lais Haughian has been taught all about fraud prevention by her banking colleagues and felt confident that she knew how to keep her money safe (Kenza Bryan writes).

When her phone went dead while she was working from home in Belfast last month, for example, she was quick to think that a fraud might be taking place.

Lais, 30, was surprised to receive a series of text messages from Three, her mobile phone company. These were PACs (porting authorisation codes), which mobile phone companies send to allow people to switch operators or change number.

She has been with Three since July and had no intention of switching so immediately contacted the company by online chat to say that she was concerned about the security of her account.

She thought that had solved it, but the next day Three sent her another message with another PAC, saying: "It doesn't have to be goodbye."

Once again, Lais (pictured above with her husband, Patrick, 35) logged into her Three account and used online chat to ask the company to secure her account and to explain that she had no intention of leaving. Again, she was sure that had solved the problem but the next

afternoon she tried to call her husband and found that the connection on her mobile had gone dead. Three told her it would investigate.

The next morning she logged on to online banking and saw that someone had moved £500 from an account she uses to pay bills into another account registered under her name. The fraudster had then emptied the second account, including a £3,500 overdraft, by setting up three standing orders due to leave the same day.

When she called Lloyds, it told her she had been the victim of a Sim swap, where fraudsters hijack your mobile phone account and then use internet banking to authorise payments.

Lloyds Bank has agreed to pay Lais back, and Three has provided her with a new Sim card. Three said: “In Ms Haughian’s case, human error resulted in an oversight on her account. We sincerely apologise for this and will be contacting Ms Haughian to discuss her options.” It has sent her a letter of apology, £300 in compensation and a Christmas hamper.