YOUR GUIDE TO AVOIDING COMMON SCAMS | FRAUD AWARENESS WEEK

Scamwatch

What would you do?

Take this quiz to see how well you might spot or deal with a scam.

1. **You receive a letter telling you you've won a loyalty prize (that you never entered) for shopping in a store. You are advised to contact a claim agent immediately. What do you do?**
   a. Contact them at the phone number provided.
   b. Destroy the letter.
   c. Google the company name.

2. **You've got mail personally addressed to you from a travel agency which you've never heard of or used. There is a scratchie card attached for a competition to celebrate their 12th anniversary. When you scratch it you see you've won 2nd prize. What do you do?**
   a. Read the terms and conditions. Winners are required to provide contact details so you fill in the form and send it back.
   b. Go to the website to check it out and send them an email to check out if it's for real.
   c. Throw the mail away.

3. **You've got an email from your bank saying your account has been locked. There is a link provided to unlock it. What do you do?**
   a. Click to unlock it – They've got my email address and the email looks legitimate.
   b. Call my bank to check if it's true or visit the bank's official website.

4. **Inland Revenue calls to tell you that you're being investigated for a tax refund. They want you to confirm your name and IR number. What do you do?**
   a. Ask them for their name and number, note it down and then provide your contact details.
   b. You're not sure who you're talking to. So you hang up and contact Inland Revenue on a publicly listed number or visit their official website.

5. **A professional sounding person from an investment trading company calls you about the opportunity to purchase shares in a well-known international company before the shares are made available to the public. They direct you to their polished website and to media stories about the share offer. What do you do?**
   a. Check their website to see if they are regulated in New Zealand.
   b. Google search their key personnel to make sure they seem legitimate.
   c. Hang up.

Answers

1. B – As a general rule, if you haven't entered a competition, there's no way you can win one. Scammers are very clever and change their names frequently so not finding a record of them doesn't mean they are legitimate. Providing them with your information means you could be targeted with more scam offers.

2. C – Just because something is personally addressed to you doesn't mean it's legitimate. Names and addresses are harvested by spyware, social media or simply a phone book. The website might look familiar but chances are it is fake – and never give away personal details to someone you don't know.

3. B – Scammers get email addresses from many places and their emails and websites look very authentic. Don't click on any links or attachments without checking with your bank first – you may end up with a virus on your computer.

4. B – Always be suspicious of anyone asking for personal information and don't provide any details before checking out who you are speaking to. There's nothing wrong with taking their name and number and calling them back later.

5. C – It's illegal to sell financial products by cold calling in New Zealand. Don't engage with these callers – they are extremely sophisticated and trick even experienced investors. While their websites may look legitimate, they are likely include false information created by people with stolen identities.

Consumer Protection

scamwatch.govt.nz