



TOP 5 TIPS TO AVOID E-MAIL FRAUD

Learn how to spot e-mails that'll leave you broke and feeling like a victim

Almost the moment e-mail was invented, criminals began using it to rip people off. Over the years, they've gotten good at it. We don't know exactly how good as most victims are too embarrassed to file a complaint. Of those who have come forward, the losses run in the tens of millions of dollars.

The Ontario Provincial Police and the Canadian Anti Fraud Centre say last year, one scam alone, the "emergency scam" was reported 225 times and was successful 61 times with victims defrauded of more than \$230,000. The emergency scam involves an e-mail from a relative or friend whose e-mail account has been hacked, claiming to be in dire straits and asking for money. This is only about 5% of frauds reported.

Top five ways to protect against e-mail fraud

1) If you don't know who sent the e-mail, don't open it. Fraud occurs in two ways: Win your trust and confidence in order to convince you to hand over money, credit card information or personal information. Clicking to open an attachment can install a program in your computer that will spy on your activities and report back to the sender with information on what websites you go to and what your passwords are.

2) If it sounds too good to be true it probably is. The classic Nigerian bank scam (we'll pay you a large sum if you help get money out of the country, but we need a small deposit first) and someone claiming to be a hit man hired to kill you but will reconsider if you pay him off.

3) Even if e-mails look legit, they're probably not if they're asking you to reset your password. It looks like a Facebook e-mail about resetting your password or someone wanting to "friend" you, but look closely and compare it to a real Facebook e-mail. Look at the different URLs. They want to take you to a "look alike" website where they'll phish your sign in and hack your account or trick you into downloading malware. Similar e-mails mimic eBay, PayPal and most Canadian banks.

4) You're not going to win a lottery you never entered. Banks, governments, schools, credit card companies, lotteries and courier companies do not mail you about lost money accounts, tax refunds, undelivered packages or your account status. They're all Phishing for the same thing: information. Hackers prey on your greed and know that a large tax refund or an unexpected package from a long lost rich relative is just the thing to get your attention and your information.

5) Buying prescription drugs from an unsolicited e-mail is the fastest way to get a fraud related headache. Viagra, Cilais, Levitra and the like are expensive when you buy them legitimately - but those e-mails offering rock-bottom prices? Forget it - It is a scam. All they will give you is a headache!!