INFORMATION SECURITY OFFICE

Top six ways to spot a phishing attack

What is phishing and how can we spot it?

Phishing is an attempt, usually through email, to gather personal information or to compromise technology for the purpose of financial gain or malicious activities. Phishing emails typically include a link to a fraudulent site or an attachment containing malware. Every day, millions of phishing emails are sent out to unsuspecting victims all over the world. Some are easy to detect as frauds but others can be much more convincing. How can you tell a real email from a scam one? It can be tricky to do, there is no magic bullet for detecting them, but we all need to take responsibility for keeping the company safe and that means learning how to identify phishing attacks because the best way to avoid being hooked by a scam is to be prepared for it.

1 **The message has a suspicious/mismatched URL:** If you are at all suspicious, always check the integrity of any embedded URLs. Phishing message URLs may seem to be perfectly valid but if you hover your mouse over them you can reveal the true destination address.

2 **It has poor spelling or grammar:** When a major organization sends out a message on behalf of the company, the message is usually checked for spelling, grammar and legality. If a message is filled with spelling mistakes it probably didn't come from a major corporation's legal department, but remember, not all phishing emails will have these kinds of mistakes.

3 **It asks for personal information like passwords:** No reputable company will ever ask you to send or confirm passwords or logon details via email or get you to click on a link to visit a website and log-in there. If you are in any doubt if the email is genuine, find the official company website or contact information number.

4 **You are not expecting anything from the sender:** You won a big prize or competition! But did you, in fact, enter one? A financial company is 'replying' with the spreadsheet you requested, but did you ask them for anything in the first place? Chances are, this is a phishing email.

5 **You must act now!** Messages that say you must 'Reply Now' to avoid losing money or having your access cut off or account deleted are usually trying to get you to act without thinking. Take your time and investigate, don't feel rushed into doing something you shouldn't. Phishing emails often come with an excuse for you to act as quickly as possible, so you don't have time to think.

6 **Something just seems wrong:** It would be fantastic if we could cover every way a phishing attack could happen here, but the truth is the best defense we have against fraud is our common sense. Sometimes, things just don't quite seem right, learn to trust that feeling. A phishing attack is a form of social engineering, they are playing with your mind so stay alert.

If you think you have identified a phishing email, take action

Don't open the message and delete the message permanently (and delete from the deleted items).
You can confirm with Fidelity if the message originated from us by contacting FICCustService@fidelity.ca.

FCAN-1014049 09/22