Email fraud and how to avoid it

[CIBC Private Wealth logo]

[Soft music plays]

[A woman looking at a laptop]

[Email fraud and how to avoid it]

Email fraud is common, and we're all targets. This widespread criminal industry has totaled over 4 billion dollars in misappropriated funds.

[Animated numbers increasing from about $3,900,000,000 to about $4,200,000,000]

[Source: Federal Bureau of Investigation, 2020 Internet Crime Report]

It usually happens in one of two ways:

Firstly - False email accounts.

[A still image of a man looking at something on a tablet]

[1. False email accounts]

A fraudster creates a false email account to look like a trusted person or company.

[An icon of the head of a robber, with an arrow pointing at an envelope with a piece of paper with the of the robber on it.]

Their goal is to access your private information, to access your money.

[An email inbox. One email is highlighted – the sender is 'Revenue Agency', and the subject reads: 'Urgent: Please confirm login credentials'.]

For example, you may get an email or text about an incoming Interac eTransfer.

[A text message on a phone, reading: 'Hi Cindy, click the link to accept your e-transfer: bit.ly/1sNMQw]

You click on the link and get sent to a fraudulent webpage.It looks like the real thing, but it was created by the fraudster. You input your card number and password.

[A homepage for a banking website. In a blank field for 'Card number', a card number appears. In a blank field for 'Password', a password appear.]

The fraudster then has your digital fingerprint to bypass security by pretending to be YOU. Other common misleading scams can be about package deliveries, gift cards or timeshares.

[Package deliveries

Gift cards
Timeshares]

The second way that email fraud tends to happen is an email account takeover.

[A still image of a woman looking at a computer]

[2. Email account takeover]

In this case, the fraudster hacks into a real account.

[An icon of a robber and an icon of a desktop computer. The robber icon enters into the icon of the desktop. Arrows followed by an envelope with a piece of paper with the '@' symbol inside begin emerging from the desktop.]

Once they've accessed it, they can start sending emails from that account, pretending to be the owner. And with access to all of the owner's emails, the fraudster can find sensitive information and use it to make the impersonation seem authentic. Takeovers of email accounts can happen to anyone, including trusted professionals.

[Takeovers of email accounts can happen to ANYONE]

Here's an example: you're buying a cottage, and your lawyer's email gets compromised by a fraudster, who then goes into past emails to gain information about your purchase.

[An email inbox. One email is highlighted – the sender is 'Cindy Smith', and the subject reads: 'Transfer funds for Gold Lake Cottage purchase'.]

[An email body. The subject heading, partially cut-off, reads 'RE: Transfer funds for Gold Lake Cottage purch-'. The sender of the email is Brendan Jones, brendan.jones@realestatelawyers.com. The content of the email is mostly immaterial; the gist is that this email contains information that could be sensitive.]

The fraudster then sends you an email pretending to be your lawyer, with instructions about where to wire money before the closing date. You assume it's authentic and instruct YOUR BANK to send money to the fraudster's account. And your funds become irrecoverable almost instantly.

[An icon of a robber in a desktop computer, on top of which is text that reads "'Lawyer' (Fraudster)". An arrow emerging from the computer points to an envelope with a piece of paper with the '@' symbol inside. Another arrow points from this envelope to an icon of a person, on top of which is text that reads 'You'. An arrow emerges from the person icon and points to a telephone icon. An arrow emerges from the telephone icon and points to a bank icon, on top of which is text that reads 'Your bank'. An arrow emerges from the bottom of the bank icon, pointing left, back towards the desktop icon. Dollar bill icons begin emerging from the arrow and move towards the desktop icon, and eventually disappear into the desktop icon.]

Here are some tips to avoid getting hacked:

Follow up with a phone call to confirm instruction details first of all with the recipient of the funds (your lawyer in the previous example) and also phone your bank.

[Tip #1
Follow up with a phone call]

[An icon of a robber in a desktop computer, on top of which is text that reads "'Lawyer' (Fraudster)". An arrow emerging from the computer points to an envelope with a piece of paper with the '@' symbol inside. Another arrow points from this envelope to an icon of a person, on top of which is text that reads 'You'. An arrow emerges from the person icon and points downwards to a telephone icon. An arrow emerges from the telephone icon and points to a person icon, on top of which is text that reads 'Your lawyer'.

Another arrow emerges from the 'You' person icon and points to a telephone icon. An arrow emerges from the telephone icon and points to a bank icon, on top of which is text that reads 'Your bank'.]

- This is especially important for emails involving large financial transactions. And be sure to use the phone number in YOUR RECORDS rather than one that is emailed to you as the number may have been altered by the fraudster. A short phone call could be worth thousands or millions of dollars.

[In illustration of a cellphone. The screen shows contacts, including 'Brendan (Lawyer)' with their phone number highlighted beneath. An email body appears beside the phone. The subject matter is mostly cutoff from view and immaterial; of primary importance is a highlighted line that reads 'To confirm, please call 516-284-3617.]

[Tip #2
Use strong passwords]

- Use STRONG passwords.

- Many of us use very 'hackable' passwords.
  - For example, 24% of people use 'Qwerty', 'password' or '123456'.
  - Avoid passwords which follow a simple pattern.
  - Use random numbers and, where possible, randomize using letters and special characters.
  - And finally: a passPHRASE is better than a passWORD.

[An account sign in screen for the fictional character Cindy Smith. An empty password field is field with several different passwords in succession, to correspond with the preceding voiceover.]

- Create UNIQUE passwords ESPECIALLY for your email account.

[Tip #3
Create unique passwords]

- Two out of three people use one password for ALL of their accounts. But this is dangerous, as most email compromises are because of re-using passwords. Keep these passwords secret; don't tell anyone or email them, not even to yourself.

[Four different account sign in screens for the fictional character Cindy Smith. Each screen uses the same password.]

[Keep passwords secret]

- And consider using a password manager. This enables unique passwords for each login and takes away the stress of remembering them all.

[A password manager webpage showing over a dozen different passwords for different purposes (for example, ‘Bank account’, ‘Personal email account’, ‘Social media account’, etc.]

[Tip #4
Think before you click!]

- THINK before you click. If you’re not sure about a link’s source, find the website separately to ensure it’s genuine.

[A homepage for a banking website.]

- Watch out for phrases like ‘unusual transaction detected’ or ‘please login.’

[An email inbox. One email is highlighted – the sender is ‘Revenue Agency’, and the subject reads: ‘Unusual transaction detected – please login’.]

- Malicious emails often sound urgent to compel you to act now. And remember: CIBC will NEVER e-mail you and ask your for passwords, social insurance numbers and other confidential information.

[CIBC will never email you asking for
passwords
social insurance numbers
confidential information]

[Tip #5
NEVER open attachments unless you’re expecting them]

- NEVER open attachments unless you are expecting them from the sender.

We hope you now better understand email fraud and how to avoid them. CIBC remains vigilant and on high alert, and we do everything we can to protect our clients.

[A montage of a variety of still photos showing different people on computers and tablets and talking on phones.]

With a little help from you, we can make sure that we’re working together to create the safest possible environment for you and your assets.

[CIBC Private Wealth logo]