Social Engineering Scams

Social Engineering is the use of expert manipulation via email, text message, phone call or even in-person encounters. It is the most common and most effective technique used by cybercriminals. Cybercriminals often use psychological manipulation to trick individuals into revealing personal information or taking harmful actions. Read more to learn how to spot red flags, what you need to know, and how to help keep yourself safe.

Most common tactics to be aware of

Fear based manipulation. Scammers often try to create a sense of fear or anxiety to influence your decision. You might receive threatening messages that appear to come from trusted authorities such as law enforcement, government agencies or financial institutions. Warning of legal action, frozen accounts or other serious consequences. These tactics are designed to make you panic and hand over sensitive information or money.

Urgency and time pressure. Fraudsters often create a false sense of urgency to rush you into making quick decisions. For example, a message may claim your bank account is about to be closed, or that you must act immediately to claim a time sensitive offer. The goal is to prevent you from verifying the information or thinking it through.

Irresistible opportunities. If something sounds too good to be true, it probably is. Scams may promise free access to premium apps, exclusive deals, unexpected prize winnings or high paying job opportunities. In exchange, you might be asked to provide login credentials, download malicious software, or share personal details.

Beware of Red Flags

- You are pressured to respond immediately or face serious penalties, without time to think it over or verify the source.
- he message uses threatening language or implies immediate legal or financial consequences.
- It threatens to suspend your account, cancel a service, or miss out on an offer if you don't respond right away.
- You are offered free products, money, or services with little to no effort required.
- You are asked to provide personal details or login credentials in exchange for the reward.

Ways to help keep yourself safe

- ☐ Pause and assess. Slow down and don't let messages of urgency influence your judgement or decision. Always take the time to review the details carefully and research the facts before you take any action. Scammers aim to get quick reactions.
- ☐ Verify the source and always be suspicious of requests asking for your personal information. Your bank will never send you an email or call you on the phone asking you to disclose personal information such as your password, one-time passcode, or credit card number. Click here to view: What RBC will never ask.
- ☐ Do not provide any Online Banking information to anyone who calls you. This includes information such as Online Banking passwords, answers to security questions, login credentials, or your client card/credit card PIN.
- ☐ Delete the email or text message immediately. If you receive a message you suspect to be spam, delete it immediately. You can help us by forwarding the phishing email or attaching a screenshot of a fraudulent text message to phishing@rbc.com.

RBC Be Cyber Aware
rbc.com/cyber