Services bancaires commerciaux RBC

# Escroqueries par usurpation d'identité bancaire

## Comment protéger votre entreprise

### Qu'est-ce qu'une escroquerie par usurpation d'identité bancaire?

Les escroqueries par usurpation d'identité commencent souvent par un appel, un message texte ou un courriel où l'escroc se fait passer pour une personne ou une entité de confiance. Les escrocs peuvent se faire passer pour des personnes en autorité, comme un policier, un avocat, un employé du gouvernement ou une entreprise légitime, en se disant un représentant de cette entité. Peu importe l'arnaque, les escrocs ont un objectif précis en tête : obtenir des renseignements personnels, confidentiels et sensibles, dans le but ultime de voler des fonds.

Les escroqueries par usurpation d'identité bancaire sont les usurpations d'identité les plus répandues. Les escrocs se font passer pour des employés de la banque en faisant une demande ou en amorçant une conversation dans le but d'obtenir vos renseignements bancaires,et d'accéder à vos comptes et/ou à votre argent.

## Scénarios courants d'usurpation d'identité bancaire

Les entreprises doivent se familiariser avec les scénarios courants d'escroquerie par usurpation d'identité bancaire pour savoir comment les escrocs peuvent tenter de voler les renseignements confidentiels et financiers de votre entreprise et vos fonds.

### Application de partage de bureau

Les escrocs appelleront et demanderont au membre du personnel (la victime) de télécharger une application de partage de bureau. La victime peut être redirigée vers un site Web frauduleux ou invitée à clavarder par l'entremise d'un faux mécanisme de soutien. Après l'ouverture de session, l'escroc empêche la vue de l'écran et effectue des opérations frauduleuses dans la session active. L'escroc demande souvent à la victime les numéros du jeton, affirmant que les renseignements du jeton sont nécessaires pour résoudre une fraude commise dans le compte. Le partage du jeton avec l'escroc lui permet d'exécuter des opérations frauduleuses.

### Usurpation de l'identité du service de la lutte antifraude ou du service de sécurité

L'escroc peut se faire passer pour un représentant du service de lutte antifraude ou de sécurité de RBC. Il informera l'employé que son compte ou son profil a été compromis et l'invitera à prendre des mesures pour se protéger. Ainsi, les fraudeurs peuvent demander aux employés d'effectuer des opérations, ou leur demander d'envoyer un avis par courriel ou un message texte qui sera ensuite utilisé pour intercepter un virement légitime et voler les fonds de l'entreprise.

RBC Les idées prennent vie ici

## Red flags

- A call, email or text message asking for card information, password(s), e-Transfer reference number or other sensitive information.
- A request to provide a one-time passcode in order to identify the staff member.
- A request to complete actions to “secure your profile”, including sending a transfer to “RBC” or a business account, and/or initiating another type of transaction.
- A request to download a remote access application.
- A call, email, or text message with minor differences in email addresses, spelling errors within the communication, or phone calls from an unfamiliar phone number.
- A caller prolongs the conversation, utilizes misdirection, and creates a false sense of urgency to pressure staff into completing their request and sharing sensitive information.

## Ways businesses can protect themselves

- If your staff receive a suspicious call, they should hang up immediately and contact RBC at the number on the back of their card or contact their relationship manager.
- Do not share token information or other sensitive details.
- Do not click on links or provide any information if you cannot confirm with certainty who is contacting you.
- Implement strong verification procedures – verify requests before taking any action, especially those involving confidential or sensitive information.
- Regularly issue and install updates on every device on your network to eliminate vulnerabilities that may be known to criminals.
- Report suspicious texts to telecommunications companies by forwarding suspicious messages to 7726 from the mobile devices on which they were received.
- Report suspicious emails that appear to be from RBC to phishing@rbc.com.

### Stop

Scammers try to gain trust and pressure staff into taking action by pretending to be the business’s bank. Stay alert for any unusual requests.

### Check

Staff should hang up and call the number on the back of the credit card or log into the business’s online banking to verify if the bank tried to reach out.

### Talk

Share the experience with other staff members. The more people become aware of schemes scammers are using, the less likely they are to fall victim.

For more information on cyber security best practices, visit rbc.com/cyber

Ideas Happen Here™



(03/2026)