Don't Be Fooled

5 Email Requests That Should Raise RED Flags

Protecting sensitive information from phishing attacks is crucial for businesses.

Here are **5 things that a legitimate business in Canada would never ask for over email to help safeguard against phishing attempts.**

1 SOCIAL SECURITY NUMBER (SIN)

Legitimate businesses in Canada would never request your SIN over email. This is highly sensitive information used for government purposes, and sharing it via email could lead to identity theft or fraud.

2 PERSONAL BANKING INFORMATION

A reputable company would never ask for your banking details, such as your account number, PIN, or online banking credentials, via email. This information should only be shared through secure channels or in person.

3 PASSWORDS

Legitimate businesses will never ask for your passwords, whether it's for your email account, social media profiles, or any other online service. Be cautious of any email requesting login credentials.

4 CREDIT CARD INFORMATION

Businesses should not request your full credit card number, CVV code, or expiry date through email. Secure payment processes should be conducted through official websites or secure payment gateways.

5 PERSONAL IDENTIFICATION OR PASSPORT DETAILS

Your passport number, driver's license, or other personal identification information should not be shared via email. This information can be exploited for identity theft and fraud.

TELECO
Integrating Technologies

To protect yourself and your business against phishing attempts, always verify the sender's identity, scrutinize email content for suspicious requests or irregularities, and avoid clicking on links or downloading attachments from unverified sources. When in doubt, contact the company directly through their official website or phone number to confirm the legitimacy of any email requests for sensitive information.

1218 Amber Drive • 345-2900 • 1-800-465-3933 • sales@teleco.ca • Teleco.ca