

Cybersecurity Tip of the week for SMBs

Appointment with a Phish

In this week's scam, you receive an unexpected appointment confirmation email from the National Bank of Canada. Since the email is sent from the bank's official email address, it appears to be completely safe. The email also alerts you to unusual activity in your account and provides a phone number for you to call to resolve the issue.

However, this is a clever scam. Cybercriminals visit the bank's actual website and complete the official "Contact Us" form. Then, they fill in the form with a fake tech support number and an alarming message about activity on your PayPal account. Once they complete the form with their false information, they receive an official appointment confirmation email from the bank, and then they send it to you. If you call the phone number in the email you receive, you'll be connected to a cybercriminal who will try to trick you into providing your personal information!

Follow these tips to avoid falling victim to this phishing scam:

- This scam isn't limited to banking institutions. Be cautious of any unexpected emails that instruct you to take immediate action, even if they appear to be from a trusted organization.
- Never use contact information in a suspicious email. Instead, visit the organization's official website directly to locate the customer support number.
- Think before you click! Scammers can abuse real organizations' web forms to send you fake messages.
-

Jerry Jones
Eastern Kansas Regional Business Account Manager
314.359.2309
Atchison, Ottawa, & Garnett Kansas



Call me today for a free review!