

KnowBe4



Security Hints & Tips

Multi-factor Authentication

What is it?

Multi-factor Authentication (MFA) is the process of verifying that you are who you claim to be when

logging in to a device or an account. If you're reading this from your work computer, you probably logged in to your computer - that's single-factor authentication. But single-factor authentication is no longer enough to keep your accounts secure. Learn more below about the various ways you can digitally authenticate your identity.

Understanding the Types of Identity Claim Factors:

- **Something you own.** This is using a mobile phone or device that you have in your possession to prove your identity. Typically, the device provides a code via an application, text message, email, or voice call. You then enter this code, and for successful authentication, your code must match what is expected by the service you're attempting to log in to.
- **Something you know.** This is something you've memorized or stored somewhere, such as a PIN. You must supply the correct PIN to log in to your device or service.
- **Something you are.** This factor is something about your physical body that cannot be

altered, such as your fingerprint or retina. Biometric scanners or readers are used to confirm you're physically the person that you're claiming to be.

Why do I need it?

In our digitally-driven world, passwords are no longer enough to keep your information safe. These days, it takes minimal effort for hackers to break into, or social engineer their way into, accounts that are only protected by passwords. Adding an extra step to access your accounts, such as entering an authentication code, means that hackers would also need to have your phone to break in.

Create an additional layer of security and make it harder for criminals to access your data by using two-factor or multi-factor authentication. Consult your IT or Security department to see if your organization has a preferred method of multi-factor authentication.

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 actually 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 the 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.

The KnowBe4 Security Team