KeyBank

What your business needs to know about phishing, smishing, vishing, and quishing

Phishing, smishing, vishing, and quishing are all types of social engineering. The difference is the medium the fraudster uses to execute the scheme. At KeyBank, we are committed to educating you about ways to safeguard your business.

What is social engineering?

Social engineering is when a fraudster manipulates someone into sending money or sharing sensitive data. They typically pose as someone from a legitimate company and create an urgent, but phony, situation, causing the victim to panic and respond before thinking it through.

What is phishing?

Phishing is a social engineering tactic conducted through email. For example, your Accounts Receivable employee receives a fraudulent email which appears to be from a client vendor, instructing them to click an embedded link to update your business's payment information. The link sends the employee to a spoofed website that captures their login credentials as well as your company's account information.

What is smishing?

Smishing is a similar social engineering scheme to phishing, but is conducted via fraudulent text messages.

What is vishing?

Vishing is conducted via fake phone calls. Fraudsters contact the victim by phone and trick them into making a payment or divulging sensitive information.

What is quishing?

Quishing occurs when a fraudster convinces a victim to scan a malicious QR code. The code directs the victim to a harmful website that installs malware and/or captures any sensitive information that is entered.

What kinds of sensitive information are fraudsters trying to obtain?

Fraudsters typically try to get victims to divulge:

- Personally identifiable data (employee or customer names, addresses, and phone numbers)
- Financial information (bank account details, employee payroll data)
- Login credentials (usernames, passwords)
- One-time passcodes

Why are social engineering schemes effective?

- The tactics can be highly sophisticated and difficult to detect.
- Fraudsters go to great lengths to impersonate trusted sources, even posing as a vendor or client with whom your company is known to do business.
- The schemes usually involve urgent situations to relay a sense of panic, causing victims to respond quickly without having time to think or verify that the message is authentic.
- It only takes deceiving one employee to make your business a victim.

How you can help protect your business

✓ Be skeptical of unsolicited messages.

If you receive an unsolicited email, call, or text, be wary and cautious. Verify the source by contacting the organization directly using a known and trusted phone number or email address.

✓ Do not click on suspicious links or scan questionable QR codes.

Avoid clicking on links in emails or texts, or scanning QR codes from unknown sources. Hover over links to see the actual URL before clicking.

✓ Use multifactor authentication (MFA).

Enable MFA whenever possible to add an extra layer of security to your accounts.

✓ Educate your team.

Ensure that all employees are aware of these scams and know how to recognize and report them.

✓ Report suspicious activity.

If you suspect a scam, report it to your IT department or the relevant authorities immediately.

✓ Monitor your accounts regularly.

Check your bank statements and account activity daily for any unauthorized transactions.

What if I find unauthorized transactions on my KeyBank account?

Call the KeyBank Fraud Client Service Center immediately at 1-800-433-0124. Dial 711 for TTY/TRS.

Where can I get more information?

To learn more about protecting your business from social engineering scams and other types of fraud, visit key.com/businessfraud.

KeyBank