AMERICAN EXPRESS

PHISHING 101

What Is Phishing?

Phishing is a common type of fraud and cybercrime where targets are contacted by email, text message, telephone, or social media. This fraud occurs when someone poses as a legitimate institution, to lure individuals into providing the following sensitive data - personal identifiable information, banking/credit card details, and passwords.

General Tips to Help Avoid Phishing Scams

- Avoid giving out personal or sensitive account information over the phone, text or email.
- Type in the company's known website instead of clicking on links provided.
- If an email, text or phone call seems suspicious, call the company directly.

Phishing Types & Warning Signs

Email Phishing

- Spelling & grammar errors in the email
- Email address doesn't match sender
- Email has a generic greeting
- Uses urgent, respond immediately, action required language
- Email request seems suspicious.

SMishing: Text Message Phishing

- There is a suspicious link in the text message.
- Claims to be a representative of your credit card or banking institution
- Message requests that you provide personal or banking information by responding to the text or clicking a link.

Phone Call Phishing or Vishing

- A phone call from the "Security and Fraud Department" of your "credit card company" or "financial institution"
- You're told your account has been flagged for suspicious transaction and you need to verify account details.
- You're asked to provide the security code on your credit card, your banking PIN or other sensitive information.

Social Media Phishing

- Friend request from someone you don't know or one from someone you're already friends with
- Posts with links requesting personal information

To learn more about email security or report a suspicious email, please visit us at americanexpress.com/phishing.