As an industry leader in fraud prevention, we want to protect your business from cybercrime, including the most common type — phishing. With phishing, you receive an email, text, call or social media request from someone posing as a legitimate organization to lure you into providing your personal, credit card or bank account data or passwords.

**Email Phishing**
- Contains spelling/grammar errors in the email
- Has an email address that does not match the sender name
- Features a generic greeting, such as “Dear Customer”
- Uses language that encourages you to respond immediately
- Seems suspicious in nature

**Phone Call Phishing or Vishing**
- Appears to be from “Security & Fraud Department,” your “credit card company” or “financial institution”
- Informs you that your account has been flagged for suspicious transactions and you need to verify or change account details
- Requests you to provide the security code on your credit card, banking PIN or other sensitive data

**SMishing: Text Message Phishing**
- Includes a suspicious link in message
- Claims to be from a representative of your credit card or financial institution
- Asks you to provide personal/banking information by responding to text or clicking on link

**Social Media Phishing**
- Includes a friend request from a stranger or someone you’re already friends with
- Includes posts with links requesting personal information

Don’t give out personal or sensitive account information over the phone, text or email.

Type in the company’s known website address instead of clicking on links provided.

Call the company directly if you receive a suspicious email, text or phone call.

Learn more about ways to protect your business at [americanexpress.com/phishing](http://americanexpress.com/phishing)