Phishing Scams

Every day, money is lost to online phishing scams. Learn how to spot shady emails, phone calls and texts by knowing the things no bank would ever ask.

EMAIL SCAMS

Email scams account for 96 percent of all phishing attacks, making email the most popular tool for scammers. Often, they will disguise the email to look and sound like it's from your bank.

Avoid clicking suspicious links

If an email pressures you to click a link—whether it's to verify your login credentials or make a payment, it's a scam. A bank will never ask you to do that. Before you click on a link, hover over it to reveal where it really leads. When in doubt, call your bank directly, or visit their website by typing the URL directly into your browser.

Raise the red flag on scare tactics

Banks will never use scare tactics, threats or high-pressure language to get you to act quickly, but scammers will. Demands for urgent action should put you on high alert. No matter how authentic an email may appear, never reply with personal information like your password, PIN or social security number.

Be skeptical of the email received

In the same way defensive driving prevents car accidents, treating incoming email as a potential risk will protect you from scams. Fraudulent emails can appear very convincing, using official language and logos and even similar URLs. Always be alert.

Watch for attachments and typos

Your bank will never send attachments like a PDF in an unexpected email. Misspellings and poor grammar are also warning signs of a phishing scam.

What to do if you fall for an email scam

1. Change your password if you clicked on a link and entered any personal information like your username and password into a fake site.
2. Contact your bank directly to notify them you may have fallen victim to an email scam.
3. If you have lost money, file a report with the local police department.
4. File a complaint with the Federal Trade Commission or call 877.382.4357.