First Neighborhood Bank

Consumer Education

Phishing Scams

Every day, thousands of people fall for fraudulent emails, texts, and calls from scammers pretending to be a bank. These are commonly referred to as phishing scams and victims can lose hundreds, even thousands of dollars.

ABA's #BanksNeverAskThat campaign seeks to turn the table on fraudsters by empowering consumers to spot bogus bank phishing scams. For more tips on how to keep phishing criminals at bay, including videos, an interactive quiz and more, visit **www.BanksNeverAskThat.com**.

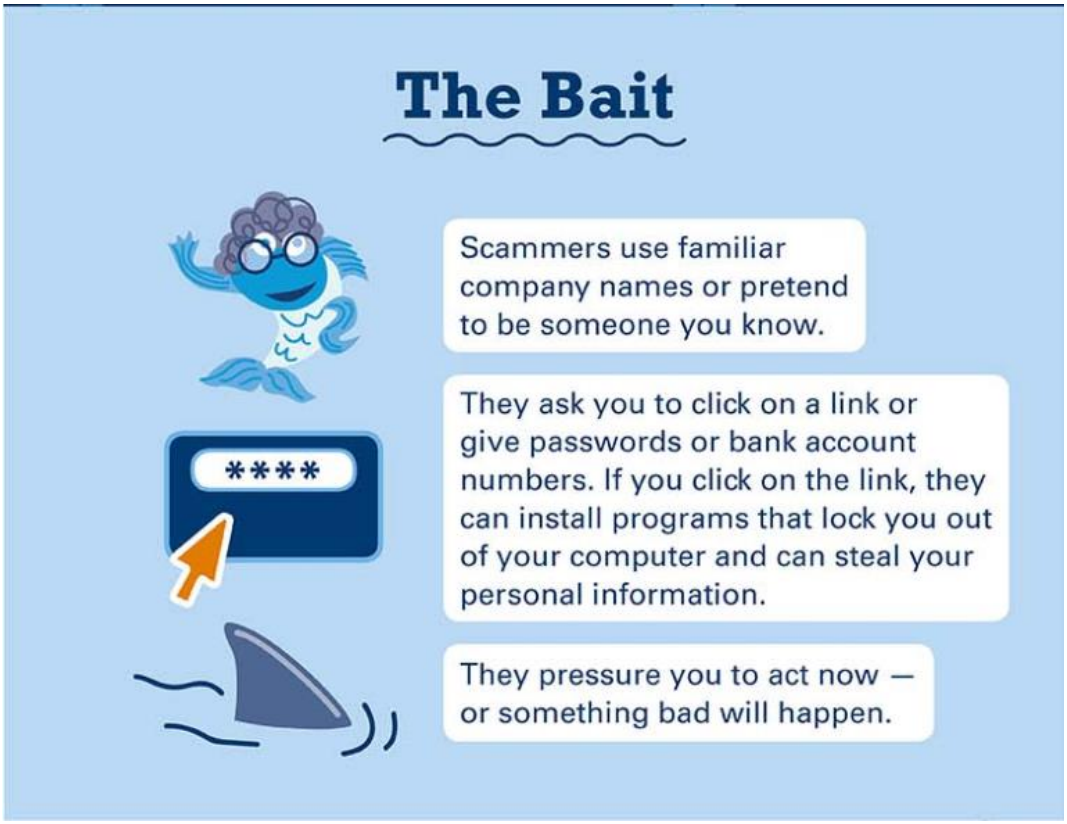
Phishing is when you get emails, texts, or calls that seem to be from companies or people you know, but they're actually from scammers. They want you to click on a link or share personal information (like a password or social security number) so that they can use that information to steal your money and/or identity.

First Neighborhood Bank

Consumer Education

The Bait

- Scammers use familiar company names or pretend to be someone you know. They send a text or 'spoofed' email or even call you in a way that makes it appear to be from a friend, family member, or an employee of a trusted organization like your bank, Credit Card Company, government agency or Phone Company.
- The bait may look and sound like a legitimate request. The scammers might even have personal information about you, like your date of birth or password.
- They often say they need your information now, to protect your account, to help a loved one in trouble, or to confirm login or password information and warn that something bad will happen if you do not act immediately.
- They ask you to give sensitive information like passwords or bank account numbers or they ask you to click on a link. If you click on the link, they can install malicious programs that can lock you out of your computer or enable them to gain access to use your personal or financial information, even from outside of the country.



First Neighborhood Bank

Consumer Education

Avoid the Hook

- Take a few minutes to check a request out. You wouldn't give your house keys to someone you don't know or trust. Don't give someone the keys to your bank account before you know who that person is and are certain that person can be trusted.
- If someone calls asking for information or wants you to act, tell the caller you will call back, then call the number on your billing statement or credit card to report the call. If the caller tries to convince you to stay on the phone, it's a scam. Hang-up and call the trusted number.
- If it's an email, don't click on it. Go to the company's website using a bookmark or type it in and check for alerts on your account.
- If you're unsure, ask a friend, coworker, family member, or caregiver to help.

Look for Scam Tip-Offs

- You don't have an account with the company.
- The email, text or caller is asking for account information, including passwords.
- Grammatical errors or something just seems fishy or not right.

First Neighborhood Bank

Consumer Education

Protect Yourself

- Keep your computer and mobile device security software up to date and regularly back up your data.
- Change your security settings to enable multi-factor authentication—a second step to verify who you are, like a text with a code—for accounts that support it.
- Change any compromised passwords right away and do not reuse those passwords for other accounts.
- Use a cloud-based account such as Google Drive or Microsoft OneDrive that can allow you to restore your data if your computer is comprised.
- Don't provide any information to anyone who calls or emails you out of the blue. Only do it if you've called or emailed them.
- Stay current on scams, check out the FTC's scam site at **https://www.consumer.ftc.gov/features/scam-alerts**.

First Neighborhood Bank

Consumer Education

Report Phishing

- Report it to the FTC at ftc.gov/complaint.
- Forward phishing emails to **spam@uce.gov** – and to the company, bank, or organization impersonated in the email. You also may report phishing email to **reportphishing@antiphishing.org**. The Anti-Phishing Working Group, a group of ISPs, security vendors, financial institutions and law enforcement agencies, uses these reports to fight phishing.
- Visit **Identitytheft.gov**. Victims of phishing could become victims of identity theft; there are steps you can take to minimize your risk.

First Neighborhood Bank

Consumer Education

For more information about phishing, visit **https://www.consumer.ftc.gov/articles/how-recognize-and-avoid-phishing-scams**

Phishing: Don't Take the Bait

The ABA Foundation and the FTC seek to raise awareness of the growing phishing threat.

Source: American Bankers Association