Fraudulent Emails, Websites and Phishing Variations

Protect Yourself

1. Do not share any confidential information through suspicious emails, websites, social media networks, text messages or phone calls.
2. Protect your personal and account information, including your online banking username, password, and answers to security questions. Do not write this information down or share it with anyone.
3. Install, run, and keep anti-virus software updated.

Fraudulent emails (phishing)
Phishing is usually a two-part scam involving emails and spoof websites. Fraudsters, also known as phishers, send an email to a wide audience that appears to come from a reputable company. This is known as a phish email.

In the phish email, there are links to spoof websites that imitate a reputable company's website. Fraudsters hope to convince victims to share their personal information by using clever and compelling language, such as an urgent need for you to update your information immediately or a need to communicate with you for your own safety or security. Once obtained, your personal information can be used to steal money or transfer stolen money into another account.

Use caution if you receive an email expressing an urgent need for you to update your information, activate your online banking account, or verify your identity by clicking on a link. These emails may be part of a phish scam conducted by fraudsters to capture your confidential account information and commit fraud.

How fraudsters obtain email addresses
Fraudsters obtain email addresses from many places on the Internet. They also purchase email lists and sometimes guess email addresses. Fraudsters generally have no idea if people to whom they send banking-related phish emails are actual bank customers. Their hope is that a percentage of those phish emails will be received by actual bank customers.

If you receive a fraudulent email that appears to come from Valley Bank, this does not mean that your email address, name, or any other information has been taken from Valley Bank's systems.

Fraudulent websites (phish or spoof websites)
Fraudsters may attempt to direct you to spoof websites via emails, pop-up windows or text messages. These websites are used to try to obtain your personal information. One way to detect a phony website is to consider how you got to the site. Use caution if you may have followed a link in a suspicious email, text message, online chat or other pop-up window requesting your personal or account information.

Variations on phishing attacks

Pop-up windows
Fraudsters may use pop-up windows – small windows or ads – to obtain personal information. These windows may be generated by programs hidden in free downloads such as screen savers or music-sharing software. To protect yourself from harmful pop-up windows, avoid downloading programs from unknown sources on the Internet and always run anti-virus software on your computer.

Telephone or voice phishing
Known as **vishing**, or voice phishing, this tactic is a phishing attempt made through a telephone call or voice message. Fraudsters may have the ability to spoof their caller ID so it could appear that the telephone call is coming from a legitimate company. Fraudsters may also have identifying customer information, such as your name, which they may use to make the call appear more authentic.

If you are uncomfortable with a phone call that was not initiated by you, hang up or ask for the purpose of the call. Then, contact the company using legitimate sources such as contact phone numbers found on the company's website, your bank statements, and those listed on your ATM, debit or credit card.

Text-message phishing
A phishing attempt sent via SMS (Short Message Service) or text message to a mobile phone or device. This tactic is also referred to as **smishing**, which is a combination of SMS and phishing. The purpose of text message phishing is the same as traditional email phishing: convince recipients to share their sensitive or personal information.

Never take action on a request for your personal or financial information, including account numbers, passwords, Social Security number or birth date. Use caution if you receive a text message expressing an urgent need for you to update your information, activate an account, or verify your identity by calling a phone number or submitting information on a website. These messages may be part of a phishing scam conducted by fraudsters in an attempt to capture your confidential account information and may be used to commit fraud.

Paper mail or fax phishing
Some fraudsters still use low-tech methods to obtain your personal and financial information. Phishing attempts can be made through regular mail or fax machines. If you are suspicious about a piece of mail or fax you have received requesting personal or financial information, you should discard it. If you've responded to a mail or fax phish and provided personal or financial information, contact the company the mail or fax appears to be from. Use a legitimate source such as the phone number listed on the company's website, billing statement, or on the back of your ATM, debit or credit card to let the company know that your information was compromised.

Reduce Your Risk

Replace paper invoices, statements and checks with electronic versions.

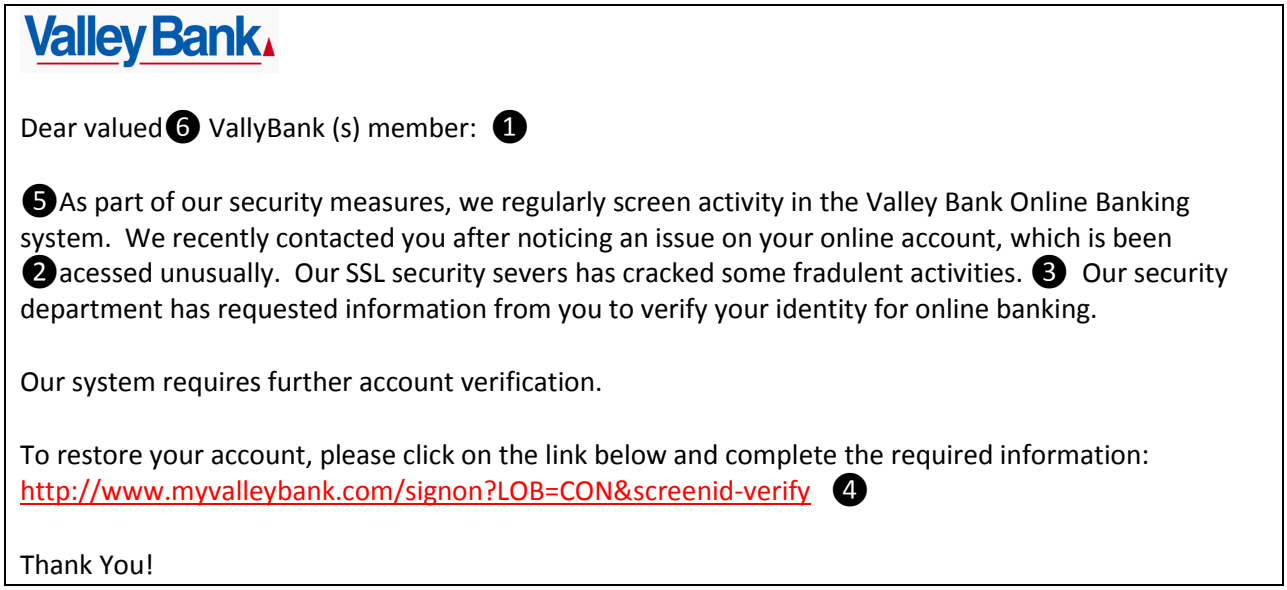
Sign up at www.myvalleybank.com for free eStatements.

Safety Tip

Never open attachments, click on links, or respond to emails from suspicious or unknown senders.

Learn to Recognize Fraudulent Emails

Fraudulent emails (phish) and websites can be very sophisticated, and may look identical to Valley Bank's emails and websites. Fraudsters can even tamper with the sender information in an email to make their phish look even more legitimate. Although fraudsters use various tactics in their phish, there are common elements you should familiarize yourself with.



1. Awkward greeting
A phish may address the customer with a nonsensical greeting or may not refer to the customer by name.

2. Typos
This is not because fraudsters do not know how to spell – it is so the phish would not be blocked by email filters.
Examples in this phish: "acessed" "Our SSL security "severs" has…" "fradulent"

3. Incorrect grammar
Another tactic used to bypass email filters.
Examples in this phish: "Our SSL security severs has…"

4. Strange or unfamiliar links
This link looks official, but what happens when the mouse cursor rolls over it. The link's source code will point to a completely different web site. Remember that you can always type a URL into your web browser instead of clicking on a link.

5. Compelling or urgent language
An urgent need to communicate with you for your own security, or a request to update your information immediately.

Examples in this phish: “We recently contacted you after noticing an issue on your online account, which has been acessed unusually.”
“Our security department has requested information from you to verify your identity for your online banking.”

6. Mis-spelled company name.
Another tactic used to bypass email filters.
Example in the phish: “VallyBank (s)”

This is not a comprehensive list of phish email characteristics, but these examples will help you learn to recognize fraudulent emails.

Valley Bank is dedicated to protecting your information. Learn about our security measures and what we do to protect your accounts online.

Report Phish and Email Scams

Send Valley Bank phish emails and fraudulent websites to:
customerservice@myvalleybank.com

If you provided personal or account information through an email or suspicious website, contact: 1-540-342-2265.

Safety Tip

Never open attachments, click on links, or respond to emails from suspicious or unknown senders.