Phishing, Vishing, and Smishing

Phishing

On the Internet, "phishing" refers to criminal activity that attempts to fraudulently obtain sensitive information. There are several ways a fraudster can try to obtain sensitive information such as your social security number, driver's license, credit card information, or bank account information, often luring you with a sense of urgency. Sometimes a fraudster will first send you a benign email (think of this as the bait) to lure you into a conversation and then follow that up with a phishing email. At other times, the fraudster will just send one phishing email.

Here are some questions to ask if you think you have received a phishing email. You can use these same questions if you receive a vishing or smishing email:

1. Do you know the sender of the email? If yes, continue to be cautious before clicking a link. If no, do not click any links.
2. Are there any attachments in the email? If so, do not click on the attachment before contacting the sender to verify its contents.
3. Does the email request personal information? If so, do not reply.
4. Does the email contain grammatical errors? If so, be suspicious.
5. If you have a relationship with the company, are they addressing you by name?
6. Have you checked the link? Mouse over the link and check the URL. Does it look legitimate or does it look like it will take you to a different Website?

Vishing

Unfortunately, phishing emails are not the only way people can try to fool you into providing personal information in an effort to steal your identity or commit fraud. Fraudsters also use the phone to solicit your personal information. This telephone version of phishing is sometimes called vishing. Vishing relies on “social engineering” techniques to trick you into providing information that others can use to access and use your important accounts. People can also use this information to assume your identity and open new accounts.

To avoid being fooled by a vishing attempt:

- If you receive an email or phone call requesting you call them and you suspect it might be a fraudulent request, look up the organization’s customer service number and call that number rather than the number provided in the solicitation email or phone call.
- Forward the solicitation email to the customer service or security email address of the organization, asking whether the email is legitimate.

Smishing

Just like phishing, smishing uses cell phone text messages to lure consumers in. Often the text will contain an URL or phone number. The phone number often has an automated voice response system. And again, just like phishing, the smishing message usually asks for your immediate attention.

In many cases, the smishing message will come from a "5000" number instead of displaying an actual phone number. This usually indicates the text message was sent via email to the cell phone, and not sent from another cell phone.

Do not respond to smishing messages.

Examples of Phishing Messages:

You open an email or text, and see a message like this:

"We suspect an unauthorized transaction on your account. To ensure that your account is not compromised, please click the link below and confirm your identity."

"During our regular verification of accounts, we couldn't verify your information. Please click here to update and verify your information."

"Our records indicate that your account was overcharged. You must call us within 7 days to receive your refund."

The senders are phishing for your information so they can use it to commit fraud.

American Bank & Trust Card Monitoring Text Sample

The below is a sample communication by TEXT from American Bank & Trust and is a VALID request for transaction confirmation from our Debit Card Fraud Monitoring Program:

SecurLOCK Communicate

SMS Samples

SMS Alert

FreeMsg: (Financial Institution Name) Fraud Dept: Suspicious txn on acct 1111: $201.99 WALMART. If authorized reply YES, otherwise reply NO. To Opt Out reply STOP.

SMS Response to "YES"

FreeMsg: (Financial Institution Name) Fraud Dept: Thank you for confirming this activity. Your account is safe for continued use. To Opt Out reply STOP.

SMS Response to "NO"

FreeMsg: (Financial Institution Name) Fraud Dept: Thank you. We will call you or you can call us anytime at 800-369-4887. To Opt Out reply STOP.

SMS Response to "HELP"

FreeMsg: (Financial Institution Name) Fraud Dept: received your msg. It is important we talk to you. Please call 800-369-4887 ASAP. To Opt Out reply STOP.

American Bank & Trust Card Monitoring Email Sample

The below is a sample communication by EMAIL from American Bank & Trust and is a VALID request for transaction confirmation from our Debit Card Fraud Monitoring Program:

From: FraudServiceCenter@FinancialInstitutionName.com
Subject: URGENT: Your Card Has Been Suspended Due To Recent Account Activity

Your Credit Card Ending in 1113

Dear (Cardholder's Name):

As part of our commitment to protecting the security of your account, we continuously monitor for possible fraudulent activity. We need to verify that you, or someone authorized to use your account, attempted the following transaction(s) on your account ending in 1113:

Merchant	Amount	Date	Time	Location
TRIGGER	$440.01	04/01/2016	08:01 AM	MILWAUKEE, WI
WALMART	$504.95	04/01/2016	10:02 AM	MILWAUKEE, WI
WALMART	$104.95	04/01/2016	09:31 AM	MILWAUKEE, WI
WALMART	$54.95	04/01/2016	09:01 AM	MILWAUKEE, WI
WALMART	$304.95	04/01/2016	08:01 AM	MILWAUKEE, WI

If the dollar amount is not identical to what is shown on a transaction receipt, this may be due to a pre-authorization which has not yet posted to your account.

The merchant location for internet transactions may be different than you expect as they are often cleared through a centralized billing location.

If you have already spoken with us about these transactions, then no further action is required.

Please click on one of the two statements below that best represents the transactions above:

All Transaction(s) Authorized One or More Transaction(s) NOT Authorized

NOTE:

Your satisfaction is very important to us and we appreciate your prompt attention to this matter. If you have any questions about the content of this email, please don't hesitate to contact us at 800-369-4887 from the U.S. and Canada. If you prefer, use the phone number on the back of your card. Internationally, you can reach us collect at 727-227-2447 and we will accept the international collect call charges. For your convenience, we are available to take your call 24 hours a day, 7 days a week.

Thank you for being a valued customer.

Sincerely,

(Financial Institution Name) Fraud Service Center

Please do not respond to this email, this mailbox is not monitored. It is only used for sending Fraud Alert Email notifications.

The previous example is a valid email – Still, if you feel uncomfortable with an email or text the safest way to deal with it is to delete it and call the bank.

How to Deal with Phishing Scams

- Delete email and text messages that ask you to confirm or provide personal information (credit card and bank account numbers, Social Security numbers, passwords, etc.). Legitimate companies don't ask for this information via email or text.
- The messages may appear to be from organizations you do business with – banks, for example. They might threaten to close your account or take other action if you don't respond.
- Don't reply, and don't click on links or call phone numbers provided in the message, either. These messages direct you to spoof sites – sites that look real but whose purpose is to steal your information so a scammer can run up bills or commit crimes in your name.
- Area codes can mislead, too. Some scammers ask you to call a phone number to update your account or access a "refund." But a local area code doesn't guarantee that the caller is local.
- If you're concerned about your account or need to reach an organization you do business with, call the number on your financial statements or on the back of your credit card.

Report Phishing Emails

Forward phishing emails to spam@uce.gov — and to the company, bank, or organization impersonated in the email. Your report is most effective when you include the full email header, but most email programs hide this information. To find out how to include it, type the name of your email service with "full email header" into your favorite search engine.

You also can report phishing email to reportphishing@antiphishing.org. The Anti-Phishing Working Group — which includes ISPs, security vendors, financial institutions and law enforcement agencies — uses these reports to fight phishing.

If you might have been tricked by a phishing email:

- File a report with the Federal Trade Commission at www.ftc.gov/complaint.
- Visit the FTC's Identity Theft website. Victims of phishing could become victims of identity theft; there are steps you can take to minimize your risk.

Enable the "block texts from the internet" feature if available from your cell provider

Most spammers and smishers send texts via an internet text relay service which helps hide their identity and also doesn't count against their text allowance (scammers are notoriously frugal). Many cell providers will let you turn on a feature that will block texts that come in from the internet. This is another easy way to cut down on spam and smishing e-mail.