Sharekhan
Your guide to the financial jungle

Customer Awareness Mail

September 2015

PHISHING..!!

Introduction

Phishing is a broad term that refers to attempts by criminals to secure personal information from online users without their knowledge or consent. Over the years, many different types of phishing attacks have emerged, and continue in common use today. In order to be on the alert for these scams, it is important to be aware of the several common strategies used as part of these attacks.

Types of Phishing

1. Phishing
2. SMiShing
3. Vishing

1. Phishing

Phishing scams are typically fraudulent email messages appearing to come from legitimate enterprises (e.g. your Internet service provider, your bank). These messages usually direct you to a spoofed web site or otherwise get you to divulge private information (e.g., password, credit card, or other account updates). This private information is then used to commit identity theft.

One type of phishing attempt is an email message stating that you are receiving it due to fraudulent activity on your account, and asking you to "click here" to verify your information.

Ways to Avoid Phishing Scams:

1. ***Guard against spam:***

   Be especially cautious of emails that

   - Come from unrecognized senders.
   - Ask you to confirm personal or financial information over the Internet and/or make urgent requests for this information.
   - Aren't personalized.
   - Try to upset you into acting quickly by threatening you with frightening information.

2. ***Communicate personal information only via phone or secure web sites:***

   When conducting online transactions, look for a sign that the site is secure such as a lock icon on the browser's status bar or a "https:" URL whereby the "s" stands for "secure" rather than a "http:".

3. ***Do not click on links, download files or open attachments in emails from unknown senders.***

   It is best to open attachments only when you are expecting them and know what they contain, even if you know the sender.

4. ***Never email personal or financial information***

   Even if you are close with the recipient, you never know who may gain access to your email account, or to the person's account to whom you are emailing.

5. ***Beware of links in emails that ask for personal information:***

   Even if the email appears to come from an enterprise you do business with. Phishing web sites often copy the entire look of a legitimate web site, making it appear authentic. To be safe, call the legitimate enterprise first to see if they really sent that email to you. After all, businesses should not request personal information to be sent via email.

6. ***Beware of pop-ups and follow these tips:***

   - Never enter personal information in a pop-up screen.
   - Do not click on links in a pop-up screen.
   - Do not copy web addresses into your browser from pop-ups.

- Legitimate enterprises should never ask you to submit personal information in pop-up screens, so don't do it.

7. ***Protect your computer:***

   Protect your computer with a firewall, spam filters, anti-virus and anti-spyware software. Do some research to ensure you are getting the most up-to-date software, and update them all regularly to ensure that you are blocking from new viruses and spyware.

8. ***Keep a Check:***

   Check your online accounts and bank statements regularly to ensure that no unauthorized transactions have been made.

2. Vishing

When you're online and somebody asks you to "update your account information", you probably don't even think twice. It's a scam 99% of the time. But what if you get a phone call? Do you assume those are fake as well?

High-Tech Scheme, Low-Tech Tool

Scammers are increasingly using a low-tech tool – the telephone – to rip people off. They can set up a system that automatically dials a long list of phone numbers and asks for account information. What's more, they can mask the number that shows up on caller ID said that the incoming call looks legitimate.

This form of fishing for valuable information is called "vishing". As you've probably guessed, it's a variation of the term "phishing" – and the V stands for Voice. We can sometimes be less guarded when a phishing attack comes through the phone lines.

Avoid Vishing - Don't Get Snagged

Beware of phone phishing schemes. Do not divulge personal information over the phone unless you initiate the call. Be cautious of emails that ask you to call a phone number to update your account information as well.

3. SMiShing:

SMiShing scams are similar to phishing scams. You get a message from a bank or service provider asking you to do something. However, the SMiShing is really a message from a scam artist.

How SMiShing Works

SMiShing scams often direct you to visit a website or call a phone number.

If you dial the number, you'll be asked for sensitive information like a credit card number.

If you visit the website, it may attempt to infect your computer with malware.

Scammers continually get more and more creative. Most consumers are savvy enough not to fall for the old "we need your bank account password" email.

However, a text message seems less threatening. Instead of just trying to get money from you, like they do in cashier's check scams, SMiShing schemes often just try to get information such as credit card numbers. Then they use or sell the information later.

Lesson to learn:

You should always be careful about giving out personal information over the Internet.

Remember that you may be targeted almost anywhere online, so always keep an eye out for those "phishy" schemes and never feel pressure to give up personal information online.