Blueprint of a Phishing Attempt

It would be helpful if content from threat actors came with a flashing red flag. Unfortunately, phishing attempts are better crafted than we'd like to believe. Cyber threat actors are well versed in manipulation and well-crafted techniques to fool unsuspecting users. When a user falls for a phishing message, the attacker achieves their purpose.

Phishing messages can appear in a variety of formats to collect personal information, steal account credentials, or install malware on a user's device. However, there are some common indicators that can be looked for in these phishing attempts. Let's take a look at some examples that highlight how to identify messages as phishing attempts and hopefully thwart this pathway for cybercriminals.

Message #1: Fake Vacation Loans

Subject: Low-Cost Dream Vacation loans!!!

Dear John,

We understand that money can be tight and that you may not be able to afford to go on vacation this year. However, we have a solution. My company, World Bank and Trust, is willing to offer low-cost loans to get you through the vacation season. Interest rates are as low at 3% for 2 years. If you are interested in getting a loan, please fill out the attached contact form and send it back to us. We contact you within 2 days to arrange a deposit into your checking account [sic].

Please email your completed form to VacationLoans@worldbankandtrust.com.

Your dream vacation is just a few clicks away.

Stephen Strange
World Bank and Trust
1818 Street, NW Washington, DC 20433 USA
www.worldbankandtrust.com

Message #2: "Amozan" Gift Cards

Subject: Free Amozan Gift Card!!!

Dear Sally,

You name has been randomly selected to win a $1000 Amozan gift card. In order to collect you prize, you need to send us your contact information so we can put your prize in the mail. This is a limited time offer, so please respond to the request within 2 business days. Failure to respond will forfeit your prize and we will select another winner. Please email your Name, address, phone # and date of birth to:

CustomerService@amozan.com

Your gift certificate is just a few clicks away

Customer Service
Amozan

What These Phishing Attempts Teach Us

In the first message, we can see that the phisher wants to give us a low-cost loan with no credit check. We just send him our information, and he gives us the money. This seems too good to be true. If you hover over the link, you see that this is not the email address displayed. It's the email address of the attacker…

In the second message, we see that "Amazon" is misspelled as "Amozan." If you read the message quickly, you will think it says "Amazon" and respond to get your gift certificate.

Here are some rules to use to protect yourself from becoming a victim of a phish:

Rule #1: If an offer or deal is too good to be true, it probably is.

Rule #2: Hover over the link to confirm its true origin.

Rule #3: Look for misspellings. If company names are close to the correct spelling, you may not initially notice incorrect spelling.

Rule #4: Type the correct URL in the address bar yourself to ensure you are going to the legitimate site.

Rule #5: Look for misspellings in URLs. Some scammers use slight misspellings or letter substitutions in web addresses so that it is not easily noticed (e.g., 1egitimatebank.com instead of legitimatebank.com).

Rule #6: Never respond to an email with sensitive personal information (birthdate, Social Security Number, etc.). There are always more secure methods that legitimate companies will use to get this information.

Rule #7: Be wary of any message that is urging you to take immediate action.

The Federal Trade Commission is the United States entity that collects scam reports and can offer assistance in the event of an attack. If you think you've been a victim of a phishing attack or have clicked on a link that may be malicious, you can report a phishing attempt online at https://www.usa.gov/stop-scams-frauds or by placing a call to 1-877-382-4357.

The information provided in the MS-ISAC Monthly Cybersecurity Tips Newsletter is intended to increase the security awareness of an organization's end users and to help them behave in a more secure manner within their work environment. While some of the tips may relate to maintaining a home computer, the increased awareness is intended to help improve the organization's overall cyber security posture. This is especially critical if employees access their work network from their home computer. Organizations have permission and are encouraged to brand and redistribute this newsletter in whole for educational, non-commercial purposes.