Spam Management/Mitigation

Spam Management and Mitigation

In this reading, you will learn about common spam mitigation strategies. Spam is defined as any unsolicited message or call that is sent to a large number of recipients. Spam is a prevalent security concern for organizations. Cybercriminals use spam to steal important information from victims. Excessive spam can slow down mail servers and even cause the servers to crash. IT Support professionals must know how to mitigate and manage spam problems.

Types of spam

There are several different types of spam. Some spam is mass marketing from legitimate businesses. Legitimate spam is simply a nuisance, especially when it is unsolicited. Other spam can be malicious and criminal.

- **Phishing emails** attempt to trick recipients into providing personal information, credit card numbers, login credentials, etc. One famous phishing racket is the Nigerian royalty scam that asks victims to help a member of a royal family to move a large amount of money out of Nigeria. The story includes an excuse for why the royal person cannot do this for themselves and needs the victim's assistance. The cybercriminal requests the victim's bank account information for the purpose of wire-transferring the fictional royal money to the victim's account. However, the cybercriminal drains all of the money from the victim's bank account instead.

Phishing emails can also include clickbait links, which offer the victims something enticing, such as celebrity gossip, tabloid scandals, lottery winnings, etc. Cybercriminals even use spam to lure in victims by appealing to people's vices. Once the recipient clicks on the emailed clickbait link, they become victim to a number of malicious attacks. The attacks can include exposure to malware, ransomware, viruses, keyloggers, trackers, information phishing, and more.

- **Text spam** is another method used by cybercriminals to send phishing scams. Text message spam is normally less elaborate than email spam. The texts often contain a brief clickbait message followed by a link.
- **Email spoofing** is a type of phishing where emails appear to be from reputable companies, like banks, well-known brand names, government agencies, charities, etc. The "From" address of spoofed emails is forged to look like it came from the reputable company. Additionally, spoofed emails often use stolen company logos, verbiage, and formatting to appear authentic. A couple of common email spoofing scams include:
    - Fake job opportunities - Cybercriminals send emails with fake job opportunities and ask victims to provide all of the personal information that is normally requested in a job application and background check. This data may include the victim's social security number, government-issued ID info (e.g., driver's license or passport), current and former addresses, current and former employers, etc. The goal of the cybercriminal is to obtain all of the information needed to steal the victim's identity.
    - Fake credit card charges - Cybercriminals send emails that appear to be purchase receipts or alerts stating a business will be charging a large amount of money to the victim's credit cards for items the victim never purchased. The goal is to get the victim to reply or call a fake customer service line listed in the email to dispute the charges. The cybercriminal, posing as a customer service representative, asks the victim for their personal and credit card information to look up the bogus charge and pretend to cancel the fake order. Then the cybercriminal will either use the stolen credit cards or sell the victim's credit card information on the black market.
- **Tech support scams** are used to trick people into creating a security weakness for cybercriminals to hijack their computers. The cybercriminals introduce themselves as technical support for Microsoft, Dell, or other well-known computer companies. They claim that the victim's computer has been sending the company alerts about some type of fictional computer problem. The cybercriminal will direct the victims to change system settings or even set up remote sessions for the cybercriminals to change the settings themselves. The changed system settings open a door for the cybercriminals to hijack the computers to steal information, install ransomware or malware, or even to use the victims' computers as a vehicle to commit other crimes.
- **Call spam or robocalls** mimic telemarketing-type calls to collect personal information, bank or credit card numbers, and other criminally useful data from victims. Robocalls are also used to test databases of phone numbers to determine which are legitimate numbers. The phone numbers that are answered by a live human are sold to telemarketers as customer leads or on the black market to cybercriminals, who use the numbers as lists of potential victims.

One of the largest spam call scams was based out of India where 700+ employees in a call center in India were arrested or detained for impersonating the United States Internal Revenue Service (IRS). This criminal organization targeted Americans with phone calls claiming that the victim owed back taxes to the IRS and must pay hundreds or even thousands of dollars immediately to avoid arrest. The criminal organization stole up to $150,000 USD per day using this extortion scam.

Spam mitigation and management solutions:

Fortunately, many cloud platforms offer services and tools to help minimize these types of attacks. The following security measures are offered by platforms like Google Workspace. Google Workspace Administration Help guides are listed with each item below. These guides provide more information, as well as the instructions for implementing these security measures in Google Workspace.

- **DomainKeys Identified Mail (DKIM):** Helps to protect victims against phishing, email spoofing, and other email spam by preventing sender address forgery. DKIM attaches a header that contains a cryptographic private key to each email sent. This key is used to verify the identity of the sender and to detect if the email message was manipulated while in transit across the internet. Receiving email servers will usually designate emails without legitimate DKIM keys as spam. For more information and instructions to implement DKIM in Google Workspace, please see the article: Help prevent spoofing and spam with DKIM
- **Sender Policy Framework (SPF):** Used to control which domains, email servers, and IP addresses can send emails for an organization. SPF is examined by the receiving email servers to verify that the domains, email servers, and IP addresses from incoming emails are from approved senders. For more information and instructions to implement SPF in Google Workspace, please see the article: Help prevent spoofing and spam with SPF
- **Domain-based Message Authentication, Reporting, and Conformance (DMARC):** Defines how the receiver should treat email messages depending on the results of DKIM and SPF checking. For more information and instructions to implement DMARC in Google Workspace, please see the article: Help prevent spoofing and spam with DMARC

Resources for more information

- Stop Unwanted Robocalls and Texts - The United States Federal Communications Commission offers tips for stopping robocalls and phone scams.
- 10 tips on how to help reduce spam - Microsoft's tips on how to handle email spam. Some items suggested are specific to Microsoft Outlook.
- How to stop spam texts: 8 do's and don'ts - Norton's advice on preventing attacks from spam texts. Some of the methods listed for combating text spam are specific to the United States.

Mark as completed