DNSFilter®

PHISHING IS ONE OF THE MOST DESTRUCTIVE INTERNET THREATS, ACCOUNTING FOR 43% OF ALL DATA BREACHES AND ACCOUNTING FOR MILLIONS IN LOST REVENUE.

The Impact of Phishing

In November 2018, Marriott revealed that their Starwood guest reservation system had been hacked. Private information for over 500 million guests was leaked in the breach. This highlights the responsibility that businesses have to keep their information secure, and the devastating consequences of a data breach.

Phishing is one of the easiest and most effective methods at gaining confidential information from individuals and businesses. Studies show that more than one in ten users who receive a phishing email will respond to it. For businesses, this represents a large and growing threat. Imagine if one of these users was an employee in your company that was responding to what they thought was a login for your company bank. What kind of sensitive information could they leak? How about your accounting data, personnel information, or trade secrets?

What is Phishing?

> **Phishing** is when someone **impersonates** a **trusted party** to give sensitive information.

More than any other type of attack, Phishing has the goal of making you believe that you are interacting with legitimate content. There is a key focus on **impersonation**. This appearance is essential into coaxing the user to input sensitive information. The software running behind the scenes is not sophisticated. All of the focus is on the visual appearance.

The second element is that of the **trusted party** being impersonated. In a broad phishing campaign, the most frequently mimicked entities are Software-as-a-Service vendors, particularly Microsoft Office 365, Google G Suite, and Dropbox. This is because they often function as authentication mechanisms for other apps.

Attacks in Contrast

Phishing is unlike other forms of computer and network attacks. Many other types of attacks are focused on inflicting harm (viruses), freezing resources for monetary gain (ransomware), or degradation of infrastructure (denial of service). Phishing has the singular purpose of extracting sensitive Personally Identifiable Information, with a key focus on authentication or payment information.

Phishing Attack Timeline

1. Target is Chosen - Phisher decides on either a broad target or narrow group for targeted Spear Phishing campaign.

2. Domain is Prepared - New domain is registered or existing site is hacked to utilize credibility. A website is setup which focuses on two key elements: appearance of legitimacy, and a functional form which captures login credentials. In 2019, SaaS applications G Suite, Office365 and Dropbox are the most imitated.

3. Phishing Package is Created - A package is created through email and/or common file such as PDF on a shared location (i.e. Dropbox). Email is the easiest and most common method of distribution. Verizon reports 92.4% of malware distributed via email.

4. Campaign is Sent - The phisher sends the package to his target list. The two most likely types of emails are programmatic (password resets, account notices) and Newsletters (product announcements).

5. User Responds - 1/3rd of users who receive phishing emails will open the email. 12% of users will click the link inside and be taken to the phishing URL.

6. Form Data Sent - Form data and metadata (IP address etc) is sent to phisher for immediate use.

6 Ways to Mitigate Phishing

What You can do

1. User Education / Fake Campaigns - User education is an essential first step in phishing mitigation. Users should be trained to visit the homepage of an application directly if they are in doubt. Platforms such as king-phisher and gophish also offer the ability to run harmless phishing campaigns on your users.

2. Implement 2FA - Two-factor authentication can help to isolate the compromise of user credentials. It is not a complete solution, since many people still reuse their password across 2FA and non-2FA sites.

3. Password managers - Password managers can limit the damage of a phishing attack to only one website, if credentials are only used for one application.

What DNSFilter can do

1. Aggregate Multiple Security Feeds - Our platform integrates multiple security feeds. This establishes a secure baseline for your outgoing network requests.

2. Domain Greylisting – Phishing campaigns are typically a fly-by-night operation. Many attacks are launched and completed within the first 30 days of a domain being registered. DNSFilter can be set to block newly registered domains so that domains are given a 30-day proving time before being accessed. This is a highly effective measure against phishing.

3. Artificial Intelligence Categorization - Our A.I. scanner is trained to detect and compare the images on websites with that of legitimate sources. For example, a Dropbox login being utilized on a non-Dropbox affiliated site. Because phishing campaigns attempt to mimic legitimate brands and companies, this is a highly effective measure at detection and access prevention. Our AI scanner also prevents your users from accessing inappropriate content by scanning and classifying unknown websites in real-time, before allowing access based on your policies.

DNSFilter®
1440 G Street NW
Washington, D.C. 20005
www.dnsfilter.com

103.247.36.36, 103.247.37.37 - AS64089