How Phishing Works – and What You Can Do About It

What is Phishing?

Phishing is a particularly malicious type of cybercrime where attackers steal sensitive information from unsuspecting victims. What distinguishes phishing from other forms of cyberattacks is that phishing emails appear to come from trusted entities. These scams are typically deceptive email messages that appear as if they were sent from a colleague or the IT department, and are positioned to extract private information like usernames, passwords, and even financial data from the recipient.

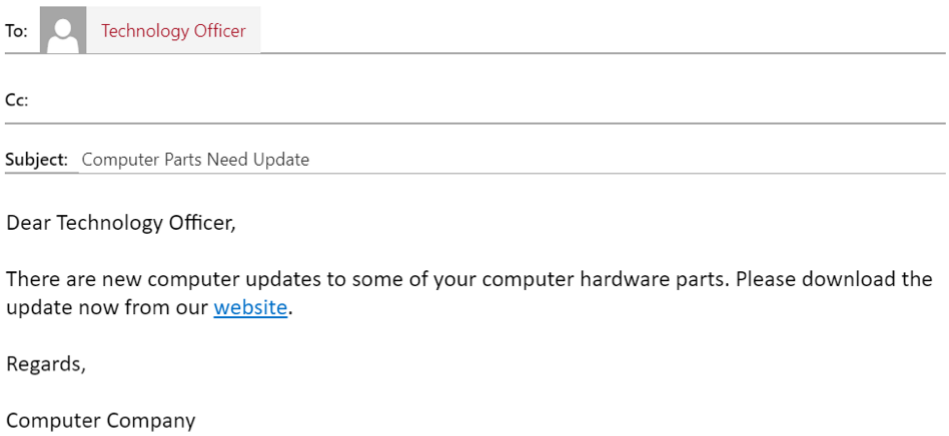
One example of phishing is an attacker who attempts to disguise themselves as being form a trustworthy company like a bank or credit card company (or any site that has login credentials). The attacker sends detailed and well-crafted emails to people within an organization, being sure to include a link to a “spoofed” version of the official company website, which is really a phantom website owned by the attacker. Once the victim visits the fraudulent website and enters account information, SSN, or other personal information, they will be exposed to downloading malware. If the attacker completed the scam correctly, the attacker obtained sensitive information without the victim knowing.

Another example of a phishing attempt is a spoofed email with the message, "You are receiving this email due to fraudulent activity on your account." Recipients that click on a link to verify their account information immediately fall into the trap.

Phishing attacks also target financial institutions. These attacks are designed to target large numbers of employees to acquire end-to-end control of financial transactions. Generally, attackers focus on small-to-medium sized banks and credit unions, which have led to hundreds of thousands of dollars in fraudulent wire transfers.

Phishing attacks directed at specific individuals or employees are known as “spear phishing”. The attacker gathers personal information, mainly through social media, to make the fraudulent email more believable and direct, which increases its possibility of success. “Whaling” is similar to spear phishing, but specifically targets executive officers or high-profile employees in a business and government, or the ‘biggest catch’ of the company.

An example of a simple phishing email is as follows:


To: Technology Officer

Cc:

Subject: Computer Parts Need Update

Dear Technology Officer,

There are new computer updates to some of your computer hardware parts. Please download the update now from our website.

Regards,

Computer Company

How Phishing Works

Phishing scams work because they induce panic in the reader. Victims tend to be more naïve when panicked about a critical subject rather than consider that they might be a target of a phishing scam. Phishing email messages have official sounding topics such as "Your Account Information Needs to be Updated." Additionally, these scams are more popular due to the availability of phishing kits on the dark web. Phishing kits enable attackers to launch phishing campaigns without complicated technical expertise.

Attackers start by cloning a trustworthy website and attaching modified scripts that are designed to steal the victim credentials once they try to log into the cloned website. Although some victims may not automatically respond to an email from their bank, they might prioritize an email from their automobile dealer about an emergency recall about their car or an email from their child's University financial center. Attackers may modify their approach depending on these factors.

It is more troublesome when the victims are users that have the privilege and administrative access within an organization. If the victim has opportunities to approve payments or authorize bank transfers and gives up their credentials to an attacker, then the imposter can use them to initiate their bank transfer. It is much worse when an attacker has identified a high-value account holder since the attack can utilize more advanced and more determined phishing method.

Phishing scams are successful about 50% of the time. The United Kingdom experienced their biggest phishing scam when the Met Police's Action Fraud unit prevented 59 million euros from being accessed by attackers who used phishing scams to obtain the information of thirty thousand bank customers in fourteen countries.

Meanwhile, the United States and Egyptian authorities charged a hundred people in 2009 for using phishing scams to steal account details from thousands of victims and transferring $1.5 million into fake accounts.

Former CEO Waltar Stephan experienced being a victim of a phishing scam the problematic way. He fell for a scam that cost the company $56.8 million because criminals who pretended to be a higher-up in the company sent an email to Stephan about a secret transaction. Unfortunately for Stephan, the Board fired him immediately.

John Podesta, Hillary Clinton's campaign chair, offered his Gmail password during the 2016 presidential election, and employees at the University of Kansas responded to a phishing email that handed their paycheck deposit information, resulting in them losing pay.

Solutions

The best way to avoid getting phished is to eliminate password authentication. The most secure way to go passwordless is with biometrics. Fingerprint biometric authentication is easy to implement and has proven to be the most effective solution for enterprise users. Convenient one-touch authentication leveraging your biometric reduces risk, enhances workflow and cannot be shared, lost or stolen.

BIO-key offers a few products that reduce the risk of Phishing attacks including our line of compact fingerprint readers that have been tested and qualified by Microsoft. These readers offers an inexpensive pathway to device sign-in and integrate seamlessly with Windows Hello for Business. For a deep biometric experience, we offer WEB-key which provides biometric authentication into customs apps. If your organization is using SAML, BIO-key offers biometric authentication into any SAML enabled app and we also offer ID Director for Windows which adds a layer of biometric authentication to Active Directory.

References:

https://www.theinquirer.net/inquirer/feature/2460065/top-5-biggest-phishing-scams/page/5

https://kb.iu.edu/d/arsf

https://www.securityweek.com/why-phishing-works-and-how-avoid-becoming-victim

https://itstillworks.com/phishing-happen-2120.html