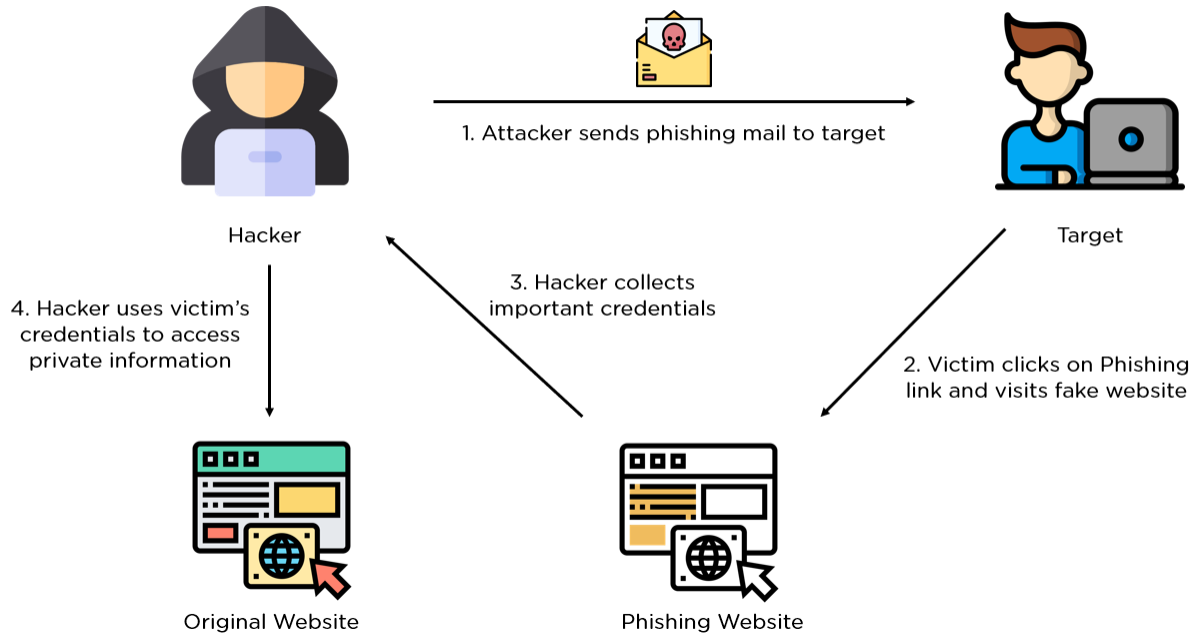
PHISHING ATTACKS

Don't get hooked



OBJECTIVES:

- Define phishing and identify various types of phishing scams.
- Recognize common baiting tactics used in phishing scams.
- Examine real phishing messages.
- Understand how to protect yourself from being hooked by a phishing scam.

WHAT IS PHISHING?

Cybercriminal attempts to steal personal and financial information or infect computers and other devices with malware and viruses.

Designed to trick you into clicking a link or providing personal or financial information. Often in the form of emails and websites. May

appear to come from legitimate companies, organizations or known individuals. Take advantage of natural disasters, epidemics, health scares, political elections or timely events

TYPES OF PHISHING ATTACKS:

MASS PHISHING ATTACK: Mass, large-volume attack intended to reach as many people as possible.

SPEAR PHISHING ATTACK: Targeted attack directed at specific individuals or companies using gathered information to personalize the message and make the scam more difficult to detect.

WHALING: Type of spear phishing attack that targets “big fish,” including high-profile individuals or those with a great deal of authority or access.

CLONE PHISHING: Spoofed copy of a legitimate and previously delivered email, with original attachments or hyperlinks replaced with malicious versions, which is sent from a forged email address so it appears to come from the original sender or another legitimate source.

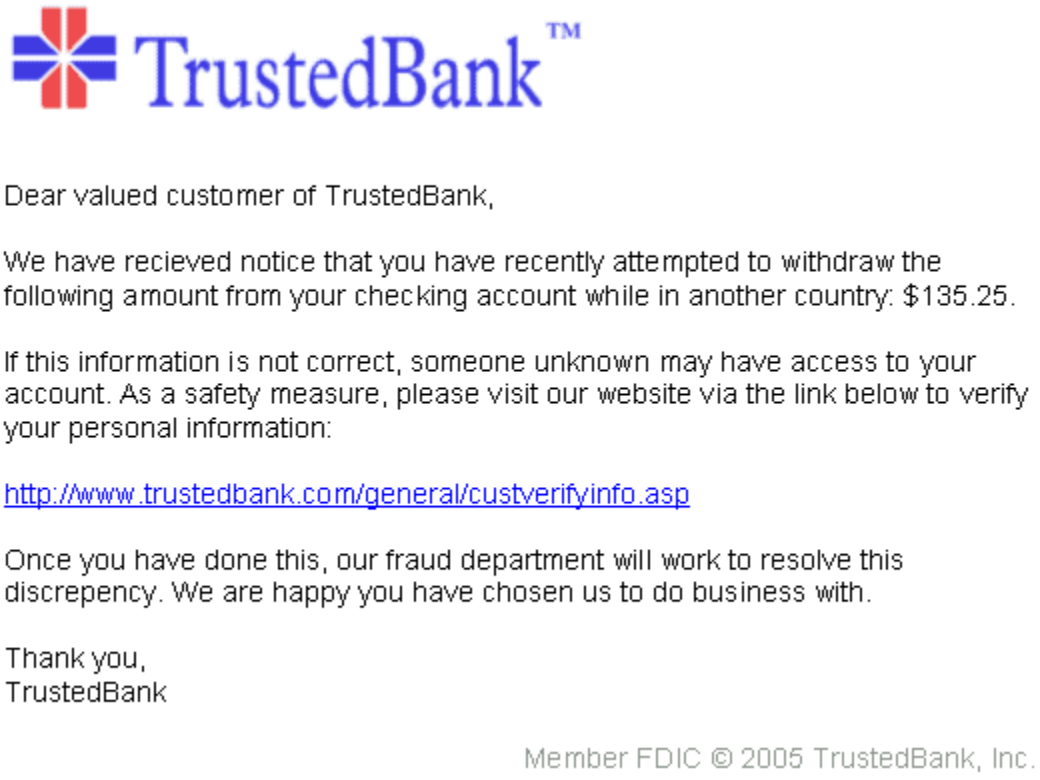
ADVANCE-FEE SCAM: Requests the target to send money or bank account information to the cybercriminal.

Techniques Used in Deceptive Phishing

Vade Secure highlighted some of most common techniques used in deceptive phishing attacks. These are as follows:

- **Legitimate links** – Many attackers attempt to evade detection from email filters by incorporating legitimate links into their deceptive phishing emails. They could do this by including contact information for an organization that they might be spoofing.
- **Blend malicious and benign code** – Those responsible for creating phishing landing pages commonly blend malicious and benign code together to fool Exchange Online Protection (EOP). This might take the form of replicating the CSS and JavaScript of a tech giant’s login page to steal users’ account credentials.
- **Redirects and shortened links** – Malicious actors don’t want to raise any red flags with their victims. They therefore use shortened URLs to fool Secure Email Gateways (SEGs). They also use “time bombing” to redirect users to a phishing landing page only after the email has been delivered. After victims have forfeited their credentials, the campaign then redirects victims to a legitimate web page.
- **Modify brand logos** – Some email filters can spot when malicious actors steal organizations’ logos and incorporate them into their attack emails or onto their phishing landing pages. They do so by looking out for the logos’ HTML attributes. To fool these detection tools, malicious actors alter an HTML attribute of the logo such as its color.

- **Minimal email content** – Digital attackers attempt to evade detection by including minimal content in their attack emails. They might elect to do this by including an image instead of text, for instance.



Recent Examples of Deceptive Phishing Attacks

We've seen deceptive phishing campaigns make headlines in recent years. Back in July 2021, for instance, Microsoft Security Intelligence warned of an attack operation that used spoofing techniques to disguise their sender email addresses so that they contained target usernames and domains. They also displayed names to use legitimate services. Ultimately, the operation's emails used a SharePoint lure to trick recipients into navigating to an Office 365 phishing page.

On the heels of the U.S. Senate passing its $1 trillion infrastructure bill a month later, Inky spotted another phishing campaign with malicious actors impersonating the U.S. Department of Transportation (USDOT). The attackers invited recipients to submit a bid for a USDOT-sponsored project by clicking an embedded button. The button redirected recipients to a website impersonating the Transportation Department that attempted to trick visitors into handing over their Microsoft credentials.

How to Defend Against Deceptive Phishing

The success of a deceptive phish hinges on to what extent an attack email resembles official correspondence from a spoofed company. Acknowledging that fact, users should inspect all URLs carefully to see if they redirect to an unknown and/or suspicious website. They should also look out for generic salutations, grammar mistakes, and spelling errors.