TRUTH SECURITY

# Checklist: How To Prevent Phishing Attacks

## The Problem

Malicious attackers are using sneaky tactics to target us as we work from home due to Covid-19. Email, voice calls/messages, and text messages are some of the popular vehicles for phishing attacks. Scams and impersonation attacks are likely to increase.

The best approach is to understand how the attackers attack then you'll be prepared to spot these attacks and defend yourself from them.

Email is still the most common method for phishing attacks, but beware of voice calls, voice messages, text messages, chat messages, social media links, and any other form of communication. Malicious attackers will use any vehicle they can.

## The Checklist

Here are several tips to help better protect yourself from common phishing attacks.

- ❑ **Beware of messages claiming to be from government officials (U.S. Centers for Disease and Prevention, CDC, World Health Organization, WHO, etc.) offering a Coronavirus Disease (Covid-19) stimulus check**. Scam monetary offers like this are common amongst attackers. Avoid clicking links, downloading attachments, or calling phone numbers in emails you receive.
- ❑ **Beware of messages asking you to click a link then enter your personal information** such as login credentials, social security, number etc. Malicious attackers are using multiple approaches to steal your information.
- ❑ **Beware of phony websites** selling Coronavirus Disease (Covid-19) testing kits or protective supplies.
- ❑ **Beware of spoofing emails** where attackers send emails that appear to be from someone they are not. These emails usually appear to be from authoritative organizations, coworkers, your CEO, etc.
- ❑ **Beware of mobile apps that track the Coronavirus Disease (Covid-19)**. Attackers are likely to create malicious apps and websites to take advantage in this climate.
- ❑ **Always connect to your corporate network via a VPN service.** This is standard for many organizations. Your IT staff will help you with this.
- ❑ **Beware of wire fraud attempts.** It's recommended that you have a multi-step approval process in place before placing any wire transfers. Common approaches are to make a phone call to the person in charge of wire transfers in your organization to make certain it's genuine and not a scam.
- ❑ **Beware of gift card scams.** Gift card scams are increasingly popular amongst attackers. They often arrive in the form of an email from your CEO or high ranking official asking you to purchase a gift card and send the info back to them via email.
- ❑ **Always verify!** A good rule of thumb is to ask before clicking on any links or responding to a message. Don't respond to a suspicious email via your email for example. Pick up the phone, send a text, etc.
- ❑ **Additional tips:**
  - ❑ Use a password manager to protect your passwords from attackers.
  - ❑ Don't reuse passwords across your accounts.
  - ❑ Use multi-factor authentication on your email, and your other logins if you are not already. Multi-factor (MFA) prevents a malicious actor from logging into your accounts even if they have your user name and password.  Examples are: Google

authenticator, a text message with a code, facial recognition, etc. You can learn more on the NIST.gov site here.

- ❑ Use your mobile phones cellular data to connect to sensitive accounts when working from home or out of the office. Wi-fi is often not as secure as your cellular data connection. Note: Nothing is 100% secure.
- ❑ Make sure your antivirus/antimalware software is running and up to date.

## Conclusion

This checklist will help you better protect yourself from malicious attackers.

New phishing attacks are popping up daily so be cautious and suspicious of every message you receive. Always verify before taking action and remember, don’t verify by directly responding to the message in question.

Use another form of communication and make certain you are speaking to the person you think you are. Malicious attackers can be very skilled Con Men. We feel it's better to be safe than sorry.

If you have further questions please don’t hesitate to contact us. (Contact info below.)

Jeremiah Baker

Cyber Security Speaker & Consultant

617-872-2875

jbaker@boninbough.com

TS TRUTH SECURITY

Disclaimer: This article is for information/educational purposes only.