CyberSecurity Spotlight

Presented by the Division of Technology & Innovation
On Behalf of the Clerk of the Superior Court for Maricopa County

Tuesday, May 3, 2022

Welcome to the premier edition of the DTI CyberSecurity Spotlight. This newsletter is intended to bring awareness to various cyber security threats and to provide education on cyber security topics.

In this premier edition, the spotlight is on a security threat called Phishing. Below, we define the term Phishing and list the various types of Phishing techniques that are used to gain sensitive information. In upcoming issues we will be providing examples of phishing emails and the process to report suspicious emails to the appropriate authority.

Thank you for reading and we hope you will help make this newsletter a success!

What is Phishing?

Phishing is a type of social engineering where an attacker sends a fraudulent (e.g., spoofed, fake, or otherwise deceptive) message designed to trick a person into revealing sensitive information to the attacker or to deploy malicious software on the victim's infrastructure like ransomware. Phishing attacks have become increasingly sophisticated and often transparently mirror the site being targeted, allowing the attacker to observe everything while the victim is navigating the site, and transverse any additional security boundaries with the victim. As of 2022, phishing is by far the most common attack performed by cybercriminals, with the FBI's Internet Crime Complaint Centre recording over twice as many incidents of phishing than any other type of computer crime.

Types of Phishing

- **Email phishing**: Most phishing messages are delivered by email, and are not personalized or targeted to a specific individual or company. This is termed "bulk" phishing.
- **Spear phishing**: Spear phishing involves an attacker directly targeting a specific organization or person with tailored phishing communications.
- **Clone phishing**: Clone phishing is a type of phishing attack whereby a legitimate, and previously delivered email containing an attachment or link has had its content and recipient address(es) taken and used to create an almost identical or cloned email.
- **SMS phishing**: SMS phishing or smishing is conceptually similar to email phishing, except attackers use cell phone text messages to deliver the "bait".
- **Page hijacking**: Page hijacking involves compromising legitimate web pages in order to redirect users to a malicious website.
- **Calendar phishing**: Calendar phishing is when phishing links are delivered via calendar invitations.

With this basic information we hope you will find it easier to spot misleading and false information.

For questions or concerns

Please email the DTI CyberSecurity Team for assistance at DTICyberSecurity@maricopa.gov.

Looking for Prior Spotlight Editions?

Prior editions can be found at the DTI CyberSecurity Spotlight page on Clerk Connect.

Copyright © 2022 Clerk of Superior Court