Phishing: Avoid Getting Hooked

Mobile devices can be protected from phishing attempts. It isn't just desktops and laptops that can have this level of protection. And the National Cybersecurity Center of Excellence (NCCoE) has developed guidance and example solution architectures to help you protect your organization's mobile devices.

Mobile Device Phishing

Phishing attacks are a persistent cybersecurity threat against organizations. Furthermore, phishing attacks no longer target only desktops or laptops. Mobile devices are now a prime target as well that require careful attention.

When individuals are "phished," they are tricked into disclosing sensitive personal information through deceptive computer-based means. Typically, a successful phishing campaign leads to an individual's credentials being stolen and then used for unauthorized access to data.

Protecting users and their devices from the risks of being phished is important. Devices with access to organizational data can be at risk of being phished and then compromising an enterprise's networks and information.

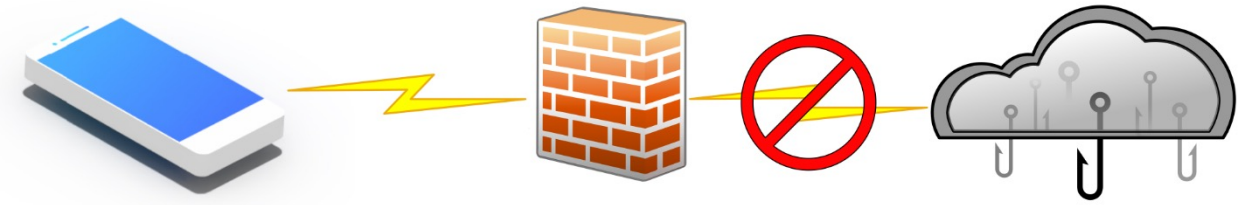
How does this happen? Malicious actors may create fraudulent websites that mimic the appearance and behavior of legitimate websites. After receiving a phishing message over email or short message service (SMS), users may then attempt to visit the website and enter their organizational credentials. This can lead to the compromise of an enterprise's networks and information.

How to Protect Your Mobile Devices

Phishing protection can be implemented on-device or at the network perimeter by organizations, sometimes using their already existing network infrastructure. The National Institute of Standards and Technology's (NIST) NCCoE developed an example solution architecture that helps enterprises protect against phishing threats for mobile devices.

Phishing: Avoid Getting Hooked

Example Solution: Minimizing Phishing Risks



The image above showcases how example solution architectures in both NIST Special Publication (SP) 1800-21 and NIST SP 1800-22 use a firewall with dynamically updated denial listings to block mobile devices from accessing known phishing websites.

The enterprise's security architecture then works to block the user's device from browsing to known malicious websites. This level of protection will help prevent the inadvertent exposure of an organization's user IDs and passwords.

In addition to URL filtering, multi-factor authentication and mobile threat defense can help protect against phishing attacks. In environments that use multi-factor authentication, if a phishing attacker successfully gains a user's password, they can still be denied access to enterprise information because they do not have the second factor required for authentication. And for environments that have protection capabilities on their devices—such as mobile threat defense--the risk of a successful phishing attack can be reduced.

For more information on phishing protection and other mobile device security and privacy enhancements for your organization, refer to NIST Special Publication 1800-21 and 1800-22.