Brand Impersonation:
What it is and how to avoid it

Email phishing attacks continue to be a growing problem as fraudsters engineer more sophisticated scams. **Brand Impersonation** phishing schemes are an offshoot of the typical Business Email Compromise (BEC) scam. Instead of receiving an email from a trusted individual inside your company like standard BEC scams, the recipient receives an email that appears to have been sent by a trusted company. One of the latest scams making its way around involves impersonating electronic signature capture company DocuSign, however, Microsoft and Apple continue to be some of the most impersonated brands.

With brand impersonation email scams, fraudsters send spoofed emails to their target that appear to be from a legit and recognizable company. These emails are typically meant to trick the target into clicking on links within the body of the email (like password reset URLs) as an attempt to collect passwords, emails, and usernames. Captured credentials are then used in **credential stuffing**, a type of cyberattack where websites are automatically bombarded with login requests using thousands of stolen credentials in an attempt to gain access to a user's account on another digital platform. These types of attacks are successful when targets recycle usernames and passwords across multiple web applications.

How can you tell if that email you received is real or not? Spoofed emails may contain some of these red flags:

- Contain spelling errors and/or bad grammar
- Sense of urgency to login via the link within the email
- Generic greetings
- The sender's email address has been altered
- Requesting that you give, confirm or update sensitive information

If you receive one of these phishing attempts, remember these tips:

- Don't click on any links within the email.
- Do not open any attachments contained within the email.
- If the request is asking you to log in with your credentials, go directly to the website to do so.

What should you do to avoid becoming a victim? See our recommendations below:

- Train employees to identify these scams and conduct testing to assess the effectiveness of your training.
- Implement spam filtering on inbound email to block unsolicited email that may contain malicious URLs.
- Automate scanning of attachments and URLs within email in a Sandbox before delivering to your corporate email system for Zero Day malware detection.

Fraudsters are constantly looking for new and different ways to deceive us. Educating your employees on these types of threats is your best defense. Staying curious with all emails received will help to ensure you're communicating and doing business with the correct person.