LIterature survey

Shortened link: Make sure that the link is in its original, long-tail format and shows all parts of the URL.

Hypertext: These are “clickable” links embedded into the text to hide the real URL.

Abnormal request: Look out for internal requests that come from people in other departments or seem out of the ordinary considering job function.

Shared drive links: Be wary of links to documents stored on shared drives like Google Suite, O365, and Dropbox because these can redirect to a fake, malicious website.

Password-protected documents: Any documents that require a user login ID and password may be an attempt to steal credentials.

Legitimate information: Look for contact information or other legitimate information about the organization being spoofed, then look to identify things like misspellings or a sender email address that has the wrong domain.

Malicious and benign code: Be aware of anything including code that tries to trick Exchange Online Protection (EOP) such as downloads or links that have misspellings.

Shortened links: Do not click on any shortened links because these are used to fool Secure Email Gateways.

Fake brand logo: Review the message for any logos that look real because they may contain fake, malicious HTML attributes.

Little text: Ignore emails that have only an image and very little text because the image might be hiding malicious code.

Notifications: Be wary of notifications that indicate being added to a post because these can include links that drive recipients to malicious websites.

Abnormal direct messages: Be on the lookout for direct messages from people who rarely use the feature since the account might be spoofed, or fraudulently recreated.

Links to websites: Never click a link in a direct message, even if it looks legitimate, unless the sender regularly shares interesting links this way.

“Unsecure”: Be wary of any hotspot that triggers an “unsecure” warning on a device even if it looks familiar.

Requires login: Any hotspot that normally does not require a login credential but suddenly prompts for one is suspicious.

For users, vigilance is key. A spoofed message often contains subtle mistakes that expose its true identity. These can include spelling mistakes or changes to domain names, as seen in the earlier URL example. Users should also stop and think about why they’re even receiving such an email.

Working within the cloud, Imperva Web Application Firewall (WAF) blocks malicious requests at the edge of your network. This includes preventing malware injection attempts by compromised insiders in addition to reflected XSS attacks deriving from a phishing episode.

Imperva Login Protect lets you deploy 2FA protection for URL addresses in your website or web application. This includes addresses having URL parameters or AJAX pages, where 2FA protection is normally harder to implement. The solution can be deployed in seconds with just a few clicks of a mouse. It doesn’t require any hardware or software installation and enables easy management of user

roles and privileges directly from your Imperva dashboard.