Brand Impersonation

Spotting the Threat

The email threats faced by organizations today vary greatly in complexity, volume, and impact. Here we take a closer look so you can spot the threat before it harms you or your organization.

Brand impersonation is designed to mimic a familiar company or business to trick victims into responding and disclosing personal or otherwise sensitive information.

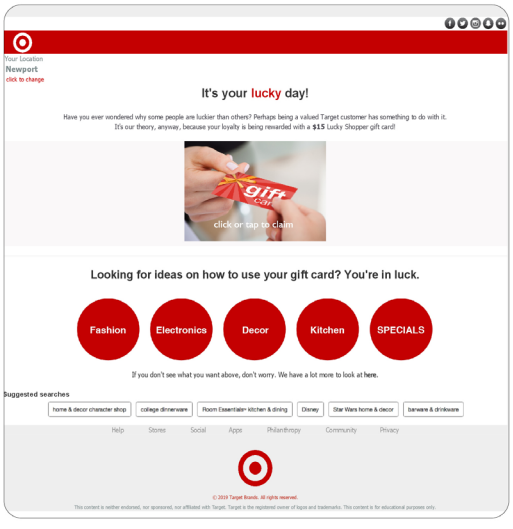
Common types of brand impersonation include, service impersonation, a phishing attack designed to harvest login credentials for personal or business accounts, and brand hijacking, whereby fake or spoofed domain names provide the illusion of legitimacy.

Brand impersonation can be difficult to detect when executed well but spoofing a brand convincingly can prove equally challenging for cybercriminals. By paying close attention to things like:

- logo use and placement
- adherence to brand colors and overall design
- copy, tone and overall content
- domain names and web addresses

You can spot irregularities and potential spoofing attempts. The sample shown indicates signs of brand impersonation.

Example



Effective brand impersonation is difficult to detect when logos and branding are mimicked properly.

Be skeptical of any offers that promise rewards or gift cards, even if the email looks convincing.

Multiple opportunities to click are common in phishing emails.

Sometimes details, or a lack of them, indicate that something's not right. Study the entire email, as well as the domain name, for irregularities.