![Barracuda. Your journey, secured.]

Domain Impersonation

Spotting the Threat

Did you know that according to the FTC, over 96% of today's companies suffer from domain spoofing attacks? Here we take a closer look so you can spot the threat before it harms you or your organization.

Attackers often impersonate domains to fool victims and carry out attacks like conversation hijacking.

They do so by using techniques such as typosquatting, replacing letters in a legitimate email domain with different ones or adding hard-to-notice characters to the legitimate email address.
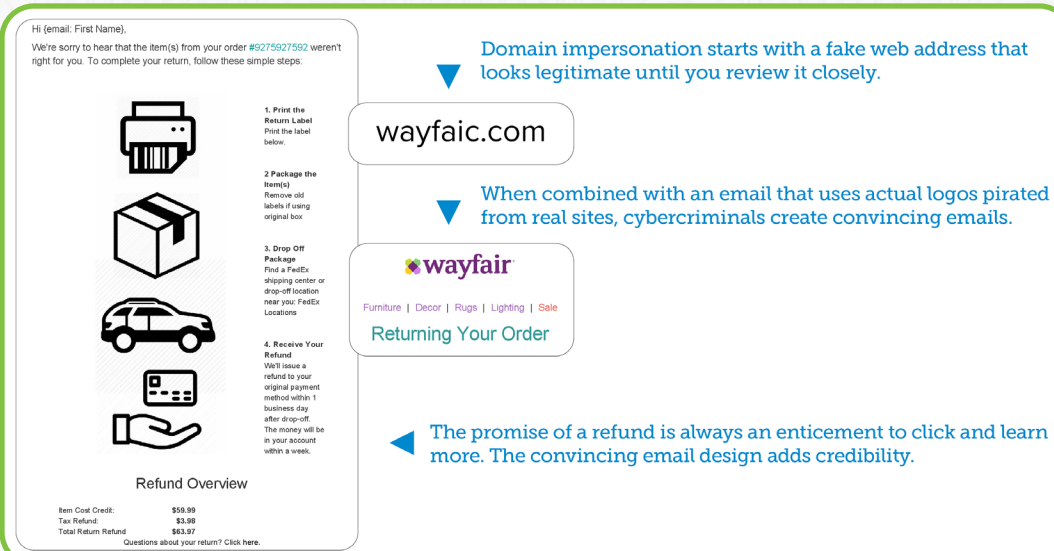
An attacker may even change the top-level domain (TLD) to .net or .co instead of .com, to fool unsuspecting victims.

In preparation for the attack, cybercriminals register the impersonating domain. It can be easy to miss the subtle differences between the legitimate email domain and the impersonator.

How to avoid becoming a victim of Domain Impersonation

• Pay close attention to domain names and web addresses.

• Be wary of hyperlinks and shortened urls, tools scammers often use to hide fake domains.

Example

Domain impersonation starts with a fake web address that looks legitimate until you review it closely.

wayfaic.com

When combined with an email that uses actual logos pirated from real sites, cybercriminals create convincing emails.

The promise of a refund is always an enticement to click and learn more. The convincing email design adds credibility.