Barracuda

PARTNER LOGO

Miss a Typo and Lose a Million!

Do you believe your eyes? Are you sure what you see is true? Many people will answer “yes” in most cases, but there are still exceptions.

A latest survey conducted by the Federal Trade Commission revealed that 96% of companies have suffered from domain spoofing attacks. What does this alarming proportion mean?

Recent years have seen many hackers impersonating the domain of legitimate business through typosquatting. They do so by replacing one or more letters in a legitimate email domain with a hard-to-notice letter, then register the impersonating domain. It is so easy for users to miss the subtle differences between fake and real domains, and unfortunately fall into the trap.

Some attackers even cleverly change the top-level domain, like using .net or .co rather than .com, which is difficult to recognize if we are not paying enough attention. By using information from compromised accounts, attackers then craft convincing messages from impersonated domains to trick victims for monetary gain, or to fulfill other malicious intentions

How to stay safe?

While ensuring that domain impersonation is part of your security awareness training for employees, it is also essential to bring in effective inbox defense technology that uses artificial intelligence to detect highly targeted attacks like domain impersonation. **Take the first step today by trying a free run of the Barracuda Email Threat Scanner.**

Scan Your Mailbox Now

Forward this to a colleague