BankOnITUSA®

INFORMATION SECURITY BRIEF

SEPTEMBER 2024

Login Here Login There; Login Everywhere

Whether you're at work, at home, or traveling, websites and applications constantly request your credentials. In today's digital world, your credentials are the key to accessing your bank software, email, insurance, streaming services, and much more. Malicious actors are eager to get that key, using various tactics to trick you and your customers into providing credentials to what appears to be a trusted site.

Here are some tips to help you assess the legitimacy of a site before logging in:

Be Skeptical of Unsolicited Links

One of the most common ways hackers steal credentials is by sending unsolicited "protected emails" that encourage you to click on a link, which leads to a fake website designed to mimic the real one. Even if the email seems to come from someone you know, be cautious, as their account may have been compromised.

Check the Website Carefully

Always compare the website URL with the real website. If you receive a link via email or text, avoid clicking it directly. Instead, manually navigate to the trusted website. Malicious actors often use website URLs that closely resemble legitimate ones. Examples include: Paypall.com, A.mazon.com, or account.microsf.com. Even a single letter can make a big difference.

Multi-Factor Authentication and Password Sharing

Where possible, always enable multi-factor authentication (MFA). We have previously written about the importance of MFA and the positive impact it has on malicious actors. In addition, avoid using the same or similar passwords for your accounts. This will significantly lessen the impact if one of your accounts was to be compromised.

The best defense against these types of attacks is your intuition. If something feels off, trust your instincts. Take an extra moment to think before entering your credentials.