FORGE

The Arkansas Cyber Defense Center

Business Phishing

A specific type of phishing targeted at businesses. The threat actor will pose as a trusted contact, such as a team member, manager, financial institution or online service provider. After gaining trust the adversary will attempt to get the victim to log into a spoofed page and steal their credentials.

Risks of business phishing:

Financial loss: An attack can lead to direct financial loss. For example, if an employee falls for an invoicing scam they may send funds to the attacker instead of a vendor or contractor.

Loss of sensitive data: If an attacker gains access to your network the may steal sensitive information such as consumer personal information or trade secrets.

Productivity loss: An attack can disrupt normal workflow and business operations.

What do threat actors want?

Adversaries typically seek login credentials in order to gain access to your system for nefarious purposes.

Red flags:

- Be very careful when clicking any links in unsolicited emails.
- You are asked to login to a system you are already be logged into.
- Email is from an unrecognized sender
- Email contains typos or grammatical errors
- Uses clever typing to disguise sender email, such as using ".corn" for .com or "goog1e" for google

POWERED BY SBA U.S. Small Business Administration

REPORT A CYBER INCIDENT:

forge.institute/acdc

501-239-9599