July 2025 Cyber Security Tip: Avoiding Phishing, Smishing, and Vishing

The Office of Cyber Security has seen an increase in texting and email scams that impersonate known business websites. Malicious actors know that it is much easier to trick humans into gaining access to systems than finding weakness in a secured network. Don't take the bait!

Phishing attacks use a practice called "website spoofing." Attackers send a malicious link to a fake website that looks just like the real thing and ask for your credentials. Once entered, attackers can use this captured information to login and commit fraudulent actions under your name.

Smishing is similar to these email scams but instead utilize text messages to persuade users to click on spoofed website links to provide sensitive information.

Vishing is another form of phishing involving a malicious actor impersonating a legitimate organization or individual over the phone to get someone to provide sensitive information.

To prevent such attacks, always double check any website links to ensure they are valid before providing any sensitive information.

Key takeaway: When receiving outside communications, be aware of the context of the messages and what you are being asked to do. If you see something suspicious, report it to **cyber.security@oa.mo.gov**.

OFFICE OF CYBER SECURITY
MISSOURI OFFICE of ADMINISTRATION