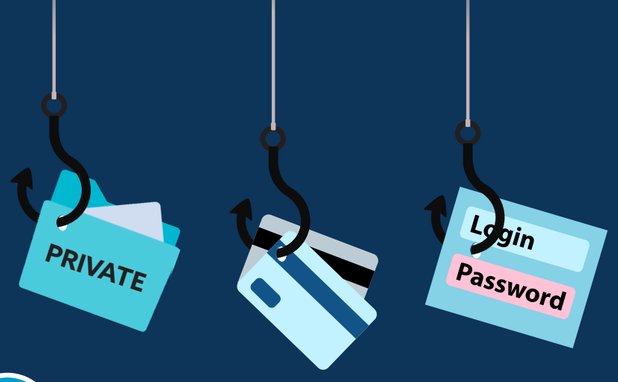
STOP PHISHING

Maine's #1 CYBER THREAT



Phishing is a form of social engineering in which a cyber threat actor poses as a trustworthy colleague, acquaintance, or organization to lure a victim into providing sensitive information or network access. The lures can come in the form of an email, text message, or even a phone call. If successful, this technique could enable threat actors to gain initial access to a network and affect the targeted organization and related third parties. The result can be a money loss, data breach, data or service loss, identity fraud, malware infection, or ransomware.

How Phishing Works



1 Urgency, Fear & Rewards

Threat actors use a sense of urgency, fear, or rewards to convince you that they are legitimate. They often pose as colleagues, acquaintances, or reputable organizations and solicit sensitive information or lure victims into downloading and executing malware.

In ME most phishing emails attempt to trick you using these typical fraud categories:

- **Change of ACH or Payment Information!**
- **Change my payroll direct deposit!**
- **Your retirement benefits are at risk!**



2 Persistent Monitoring

A phishing email is often crafted to look like it is part of a previous conversation and will include previous messages from a legitimate contact. Cyber criminals may monitor your email for up to 180 days to learn how you write, who you talk to, and what you are responsible for.

8/10 **Organizations have at least one person in a senior level position that fell for a phishing email. These emails are convincing and well written.**



3 You are the key!

Cyber criminals feed on sensitive banking information, credentials, or the ability to access files. But you are the key! Most phishing emails try to get you to type in your credentials, change banking information, or click a link that is infected. An infected link can give them remote access to your computer longterm.

70% of all attached files or links containing malware were not blocked by network border protection services

84% of employees took the bait within the first 10 minutes of receiving a malicious email

Ways to Protect Maine



IT Professionals

- **Implement strong Endpoint Software protections** — as an initial barrier to reduce the opportunity for a successful phishing attempt to further its damage.
- Configure email servers to **utilize .GOV domains, and block geographies outside of the United States.**
- **Limit internet browser variations, increase patching, and remove user administrative rights** on PCs and Laptops. This helps stop malware from installing.



Free Grant Training

- **Educate employees to recognize common indicators of phishing**, such as suspicious sender email addresses, generic greetings, spoofed hyperlinks, spelling or layout errors, and suspicious attachments. Free training is available through the MCDP Grant Process.
- **Teach employees to keep their guard up** on all communications platforms, including social media, and flag suspicious correspondence or security review.



Reporting Phish

- **Educate employees on what to do when they receive a phishing email:**
  - Report the email to the appropriate security teams.
  - Do not forward the malicious email to others.
- **Analyze reported malicious emails to prevent further intrusion:**
  - Determine if the attack was an isolated incident or company wide.
  - Identify indicators to implement within the security to prevent the attack again.



Protect Yourself

After a successful phishing attempt, the threat actors will often try to take control of its victim's account or devices to move laterally within the organization's network. To protect your network:

- **Enforce multifactor authentication** to protect from lateral movement.
- **Reduce the number of devices with access to critical data.**
- **Require complex passwords and encourage password changes on a yearly basis.** Remove non-essential elevated privileges from users.
- **Automate mandatory security updates** for browsers, applications and software on all end user devices.

Brought to you by the **State of Maine**