Security Awareness Bulletin

Utahid Phishing Attempts

January 08, 2025

Attention All State of Utah Vendors: Beware of Phishing Scams!

A recent phishing campaign is currently targeting State of Utah vendors, likely attempting to steal sensitive personal information such as passwords, credit card numbers, and other private details. This campaign is masquerading as Utahid, the system vendors use to login to conduct business with the State of Utah.

How the Scam Works:

- **Fake Emails or Texts**: The scam typically involves emails or texts claiming to be from Utahid. The message may urge you to act quickly, such as confirming account details, resetting your password, or clicking on a suspicious link.
- **Malicious Links or Attachments**: The message may contain a link or an attachment that, when clicked, leads to a fake website designed to look legitimate. These sites are used to capture personal information. Some attachments may also contain malware designed to infect your device.
- **Threats or Urgency**: Scammers often use fear tactics, such as claiming your account will be locked or your services interrupted if you don't respond immediately.

How to Protect Yourself:

1. **Verify the Source**: Always double-check the sender's email address or phone number. Official messages from Utahid will originate from utah.gov (@utah.gov) — not generic or misspelled addresses.
2. **Don't Click on Links or Open Attachments**: Avoid clicking on links or downloading attachments in unsolicited emails or texts. If you're unsure, go directly to the official website by typing the address into your browser, or contact the company directly via their known contact number.
3. **Look for Red Flags**: Pay attention to poor grammar, spelling errors, and any unfamiliar language. These are often signs of a phishing attempt.
4. **Enable Multi-Factor Authentication (MFA)**: Adding an extra layer of security to your accounts can help prevent unauthorized access even if your login credentials are compromised.
5. **Report Suspicious Messages**: If you receive a suspicious email, report it.
6. **Stay Informed, Stay Safe!**

For more information on how to recognize phishing scams and stay secure online, visit https://cybercenter.utah.gov/Cybersecurity-Tips

Stay safe online!

TLP #FFFFFF