The University of Maine

DigitalCommons@UMaine

[General University of Maine Publications](#)

[University of Maine Publications](#)

3-13-2024

Text Phishing Scams on the Rise

UMS Information Technology Services

Repository Citation

[UMS:IT Information Security Advisory] Monthly Security Update : Text phishing scams on the rise

1 message

UMS Information Security Advisory <UMS-ISO-Advisory@maine.edu>   Wed, Mar 13, 2024 at 4:40 PM
Reply-To: UMS-ISO-Advisory+owners@maine.edu
To: UMS Information Security Advisory <UMS-ISO-Advisory@maine.edu>

Dear University of Maine System Community,

We hope this message finds you well. As part of our ongoing commitment to safeguarding our shared digital environment, the Information Security Office is providing you with this monthly security update. This communication highlights the importance of staying vigilant against phishing attacks through text messaging, particularly those where the sender spoofs a supervisor or leader of the University.

Details of the Security Update:

Description: We have recently become aware of a targeted text phishing (aka SMS) campaign where the attacker is impersonating University supervisors or leaders. The attacker appears to have gathered some personal cell phone numbers from unknown sources, to make the phishing attempts more convincing.

Impact: If an employee falls victim to this phishing attack, they may inadvertently provide sensitive information, such as login credentials or personal data, to the scammer. This could lead to unauthorized access to University systems or follow-on targeted attacks.

Affected Systems: No specific University systems have been directly targeted at this time

Recommended Actions

For Everyone:

- Be cautious of unexpected text messages, even if they appear to come from a known supervisor or leader.
- Do not click on links or provide sensitive information via text message without verifying the legitimacy of the request through a separate, trusted communication channel.
- Report any suspicious text messages to the Information Security Office immediately.

For Faculty/Staff:

- Verify any unusual requests from supervisors or colleagues through a separate, established communication channel, such as a phone call or in-person.
- Be aware that these attempts are prevalent and have been on the increase recently.

For Students:

- Be aware that phishing attacks can target anyone, including students. Remain cautious of

       unsolicited text messages requesting sensitive information.
- If you receive a suspicious text message claiming to be from a University employee, report it to the Information Security Office.

Conclusion:

The Information Security Office is aware of an increase in text phishing attempts. Always be suspicious of unexpected text messages to your personal accounts that appear to be from University personnel. Feel free to report suspicious messages of all kinds, email or text-based, to the Information Security Office via phish@maine.edu.

Stay Safe,

--
To suppress notifications from this group, visit groups.google.com and search for "UMS Information Security Advisory" under "My Groups", then choose the "No email" option. Please note, suppressing notifications from this Group may keep you from receiving time-sensitive information security advisories relevant to you. If you have questions, ask at infosecurity@maine.edu. View this message at https://groups.google.com/a/maine.edu/d/msg/UMS-ISO-Advisory/topic-id/message-id