12-22-2023

End of Year Phishing Advisory and Welcome Message

UMS Information Technology Services

UMS Information Security Office

[UMS:IT Information Security Advisory] [ISO-Advisory] End of Year Phishing Advisory and Welcome Message

1 message

UMS Information Security Advisory <UMS-ISO-Advisory@maine.edu> Fri, Dec 22, 2023 at 12:26 PM
Reply-To: UMS-ISO-Advisory+owners@maine.edu
To: UMS Information Security Advisory <UMS-ISO-Advisory@maine.edu>

Dear UMS Community,

Welcome! We have created a new UMS Information Security Advisory Google Group that all active members of the UMS Community are automatically members of. The purpose of this group is to provide timely security advisories and important reminders, and we intend it to be low traffic. This inaugural email is more general in nature but we expect further emails to reflect specific, current activities. *[You can suppress notifications to this or any other Google Group you are a member of and will still be able to go back to view prior posts. See the message footer for details.]*

Again welcome, and here's our first posting to this group:

As we approach the end of the year, the Information Security Office would like to remind you to stay vigilant about phishing scams by highlighting the top phishing scams reported to us in 2023. Being aware of these scams is important for your online safety and security of your UMS and personal accounts. As you will see, some are generic to any member of the community, while others may be targeted at only students or only employees.

In 2023, over 1000 members of the UMS community exchanged over 2200 emails about phishing and other suspicious activity. The five most common scams reported to us this year have been:

1. High-Paying Remote Research Assistant Scam:

- **Scammer's method**: An email from a seemingly legitimate university address offering a remote research assistant position with attractive pay.
- **Red Flags**: The email asks for personal details and promises high pay for minimal work. Later emails from the scammer ask you to purchase office equipment upfront before a real looking (ultimately fake) check sent to you clears.

2. SharePoint Phishing Scam:

- **Scammer's method**: Emails claiming to share documents through SharePoint, often related to university services, expiring passwords, payroll changes, and updates to HR policies.
- **Red Flags**: Unexpected email invitations to access SharePoint documents.

3. E-Gift Card Scam:

- **Scammer's method**: An email from someone pretending to be a professor or your supervisor, urgently requesting the purchase of multiple e-gift cards.
- **Red Flags**: Urgent requests for gift cards, unusual email addresses, and promises of reimbursement.

4. Free Musical Instrument/Equipment Scam:

- **Scammer's method**: Offers of free instruments or tools (like pianos or TIG welders) from a faculty member, who is often "downsizing" or has a recently deceased spouse, requiring payment only for shipping costs.
- **Red Flags**: Requests for shipping fees for free items, communication outside official channels.

5. Fake Antivirus Invoice Scam:

- **Scammer's method**: An invoice for antivirus software renewal, claiming an automatic charge has been made to your account.
- **Red Flags**: Unrecognized charges, requests to update payment information via phone or email.

Please, Stay Vigilant:

- Always verify the authenticity of requests, especially those involving money or personal information. Use known-good contact information (e.g. found on vendor's official website) instead of the number found in the email.
- Consult official sources for university-related business, such as the student employment office, for student job offers.

Contact the Information Security Office if you suspect a phishing attempt (phish@maine.edu)

--