UMass Amherst
Information Technology

DON'T GET HOOKED!

HOW TO SPOT A PHISHING SCAM

Fraudulent emails will "phish" for your personal data. Do not provide personal information via email. Here are some red flags to keep in mind when opening emails from unknown senders:

STAY COOL

Often the subject line will be intended to alarm you. Watch for language warning of an account expiring, credentials needed, online money transfer needed, or security alerts.

HOW DO YOU DO?

Often the greeting will be impersonal, such as "Dear User" or "Attention email user," for example.

GRAMMAR MATTERS

Phishing emails often contain these errors throughout. Upper and lowercase letters may be used incorrectly. Symbols may be inserted at random.

STOP, THINK, ASK

The email will most likely provoke a sense of urgency, giving an imminent deadline to act. UMass Amherst IT will never threaten to suspend or terminate your account via email. Do not provide your credentials or any other personal data in response to an email message.

DO I KNOW YOU?

Phishing emails often appear to be coming from a legitimate sender. Phishing messages may pose as an internet service provider, an authority figure such as a boss or university official, or even a coworker or friend. Some scams will even use a company logo to appear more legitimate.

CLICK CAREFULLY

Watch for links or attachments within suspicious emails. Hovering over a link with your cursor will show you where the link leads to. If it is not a legitimate URL that you recognize, do not click on it. Do not download any attachments from unknown senders.

GOT HOOKED?

See back for more information.

GOT HOOKED?

WHAT TO DO NEXT

IF YOU RECEIVED A SUSPICIOUS EMAIL

Do not reply to suspicious emails, even if you recognize the sender as a well-known business or financial institution. If you have an account with this institution, contact them directly and ask them to verify the information included in the email.

Do not click any links provided in suspicious emails (or copy and paste them into a browser). They may download viruses to your computer, or at best, confirm your email address to phishers.

Do not open any attachments. If you receive an attachment you are not expecting, confirm with the senders that they did indeed send the message and meant to include an attachment.

Do not enter your personal information or passwords on untrusted web sites or forms referenced in the email.

Report any suspicious messages to **itprotect@umass.edu**.

Delete the message.

IF YOU RESPONDED TO A SUSPICIOUS EMAIL

Contact your financial institution. Don't reply to suspicious emails, even if you recognize the sender as a well-known business or financial institution. If you have an account with this institution, contact them directly and ask them to verify the information included in the email.

File a police report. Contact the UMass Police Department at **(413)545-2121** or your local police department.

Run a full virus scan regularly. To detect the latest viruses, you must use a current version of your antivirus software and keep it updated. University community members can get free antivirus from **umass.edu/it/security/antivirus**.

Update your devices' operating systems with the latest security patches - including your mobile devices. Use **Windows Update** (windows) or **Apple Software Update** (Mac) and **keep automatic updates enabled** to receive security patches as soon as they are released.

Keep your software updated, especially your web browser, mobile operating system, Adobe Reader, and Flash Player. Use **Secunia PSI** to scan for outdated software.

Only use approved storage applications for sensitive data and institutional information. Third-party applications like DropBox or a personal Google account are not appropriate storage or transmission methods for institutional information.

Do not "jailbreak" your smartphone while you are a member of the university community using the campus network.

Report phishing to **itprotect@umass.edu**

Find more info at **umass.edu/it/security/phishing**