Be suspicious of any email asking for personal information.

**DON’T FEED THE PHISH**

**Phishing:** An internet scam whereby a message is sent via email instructing recipients to immediately provide their personal account information such as passwords.

Typically, for ePanther users, these are designed to look like they came from UWM, an email service, or another service provider demanding that you “confirm” or “update” account information or passwords, or risk having an account closed down.

**TIPS FOR SPOTTING “PHISHING EMAILS”**

- **UWM will never** ask for your password.
- **Be suspicious** of any email with urgent requests for personal financial information. UWM will not email you requesting this information.
- **Never respond** directly to unsolicited emails requesting your personal information. If you think it may be a legitimate request, contact the UWM Help Desk.
- **Do not forward** the email and delete from your mailbox.
- **Do not open attachments** in emails if you are not expecting the attachment.
- **Do not click on links** in emails as the link may be an attempt to distribute viruses or malware.

If you believe you have responded to a phishing email, please contact the Help Desk.

414-229-4040 | GetTechHelp.uwm.edu

---

Phishing: An internet scam whereby a message is sent via email instructing recipients to immediately provide their personal account information such as passwords. These messages look like they came from UWM, an email service, or another service provider demanding that you “confirm” or “update” account information or passwords, or risk having an account closed down.

Be suspicious of any email asking for personal information. Never respond. Do not forward. Do not open attachments. Do not click on links.

UWM will never ask for your password.

If you think you have responded to a phishing email, please contact the Help Desk.

414-229-4040 | GetTechHelp.uwm.edu