Phishing

DON'T TAKE THE BAIT

Phishing is a kind of identity theft where hackers send you emails that imitate sites you trust, like your bank, favorite social network, or your university.

HOW IT WORKS:

MASS EMAIL
A criminal sends emails to people that appear to be from UWM or a well-known company.

MESSAGE
A phishing message will ask you to fill out a form or click on a link or button that takes you to a fraudulent website.

SPOOF WEBSITE
The fraudulent website mimics the company referenced in the email. It aims to lure you into submitting personal data.

WHAT TO DO:

- ✗ **NEVER** send your sensitive information (like your SSN) via email.
- ✗ **NEVER** give out your password.
- ✗ **NEVER** click on links in suspicious-looking email.
- ✓ **ALWAYS** check for misspelled words and poor grammar.
- ✓ **ALWAYS** verify the sender.
- ✓ **ALWAYS** beware of sensational subject lines.

Visit uwm.edu/itsecurity to learn more about phishing.

414-229-4040 | GetTechHelp.uwm.edu

UWM®