Mastodon Bytes

A new semester has begun, and so have those annoying phishing emails, unfortunately. Follow these tips on how to avoid falling into their trap!

Tip #20: Avoid Phishing Attempts

Spam email is unavoidable, but learning how to identify it when you see it will allow you to keep your information safe.

1. Identify the sender by checking the email address it was sent from. ***No* legitimate organization, including our IT Services Department, will *ever* ask for your password!**
2. Identify what the email content is asking for. **If the message seems dreamy and too good to be true, *it is!*** Pay attention to the request or message. If it says you won a million dollars or claims your account will be deleted within the next 24 hours, it seems far-fetched.
3. Check to see if the message contains grammatical or spelling errors. **Legitimate companies use proper language skills. Messages are reviewed before being sent.** If it contains misspelled words or uses improper English, it may be a phishing attempt.
4. If **your** email address is listed in the *From:* address field, the email is **fake.**

The only way to stop phishing emails from circulating is to get users to stop responding to them—**SPREAD THE WORD!**