Phishing Scams, Malicious Emails, and Other Spam

Overview

Email scams are on the rise and there is no way to effectively block them from your UWF email. In particular, a type of email scam known as phishing attempts to trick you into divulging personal information: username, password, date of birth, SSN, etc. If you responded to a phishing scam, it is important to act quickly.

The high volume of fraudulent email makes it impractical for the ITS Help Desk to alert campus of every new scam, so it is the responsibility of each UWF student and employee to learn how to identify and react to phishing emails.

If You Received a Phishing Email...

- Confirm that it is a phishing email. You can do this by identifying the signs of a phishing email (see the FAQs below). Another way to verify the authenticity of an email is by simply contacting the sender via phone or a separate email, and then asking some basic questions (e.g., "How do I know you?" and "Why may your email be important to me?").
  - The ITS Help Desk can usually trace most official emails sent by many UWF departments, if you provide the message ID (printed at the bottom of the message) or the email headers.
  - Call the ITS Help Desk at 850-474-2075 if you need help determining the legitimacy of an email or website.
    - DO NOT forward a suspicious email to anyone, not even the ITS Help Desk. If you do, then your account may automatically be flagged and locked. Instead, forward the header information.
    - Report the phishing email to Google.

If You Responded to a Phishing Scam...

- Immediately change your password or PIN, especially if you provided any sensitive data (such as a password, social security number, UWF ID number, account numbers, PINs, birthday, etc).
  - You can change your ArgoNet password via the My Account app in MyUWF (see Changing your MyUWF/ArgoNet password and Recovering Your MyUWF/ArgoNet Username or Password for more details).
  - Notify the organization that manages your account.
    - At UWF, you'll contact the ITS Help Desk (850-474-2075; helpdesk@uwf.edu).
    - Report the phishing email to Google.

Other Frequently Asked Questions

How can I identify a phishing email?

- What is the email asking you to provide? UWF and other institutions and companies will not ask you to provide sensitive data via email, and end users are discouraged from doing so.

- How urgent is the email? Scammers try to infuse their emails with a false sense of urgency (e.g., "Do this now or you'll lose your account!!!").

- What address is the email from? Official UWF emails will come from addresses ending in @uwf.edu.

- Is the email poorly written? Email scams may contain obvious typos and errors, whereas most official emails are carefully proofread.

- Does the email contain any suspicious links? Be wary of links that are misspelled, contain the @ symbol, or unusually long. In these instances, use another method to access a link (e.g., if a UWF email says to click a link that seems suspicious, log in to MyUWF or Google the link to see if you can access it that way).
Tip #1: You can check for suspicious links by simply hovering your mouse over the links. The address will appear in the bottom left of your window:

Hovering the mouse over a link will display the real URL below.

Tip #2: When checking suspicious links, be sure to check everything before the first slash (exclude http://). For example, let's examine a couple of URLs that seem to be legitimate UWF websites:

- **[http://uwf.edu/helpdesk](http://uwf.edu/helpdesk)** (all UWF websites will have `uwf.edu` before the first slash)
- **[http://learnmore.uwf.edu/](http://learnmore.uwf.edu/)** (this URL has `uwf.edu` before the first slash, and a period comes before `uwf.edu`)
- **[http://learnmore.uwf.edu/](http://learnmore.uwf.edu/)** (even though `uwf.edu` comes before the first slash, this URL isn’t valid because a hyphen separates `learnmore` and `uwf`, not a period)
- **[http://university_west_florida.com/](http://university_west_florida.com/)** (this URL doesn’t have `uwf.edu` before the first slash)
- **[http://financial-forms.com/uwf.edu/forms](http://financial-forms.com/uwf.edu/forms)** (this URL redirects to `financial-forms.com`)
- **[http://uwf.edu.free_money.com/](http://uwf.edu.free_money.com/)** (this URL actually goes to `free_money.com`, because that comes directly before the first slash)

- **Is there an alternative way to contact the sender?** Email the sender in a separate message, call the sender, or Google the sender. Ideally, the sender would include this alternative contact info in the email.

- **Does the email use specific or generic language?** Emails should contain enough specific language that a stranger couldn’t create it on their own. Senders should be sure they use specific language when sending emails, so that their recipients know that the message is legitimate.

  - **Example of specific language** – “Here are the minutes and notes from yesterday's ABC team meeting. The key takeaway is the price points for the printers.”
  
  - **Example of generic language** – “Your co-worker has shared a document with you. Click here to view it.”

  - This example is similar to the generic messages that Google Docs emails when users share documents with others. Always include your own specific language when sharing Google Docs and other files so that your recipients know that the message is legitimate.

**Can phishing emails contain official logos and images?**

Yes, phishing emails may contain official logos and images, or logos and images that look official enough.

For example, examine the [May 2017 Google Docs scam](http://example.com) that affected millions of users. It contained an official-looking Google Docs button, the email looks legitimate, and the URL for that button looks legitimate too:
But the red flags for this email are the recipients. Notice how one of the recipients is hhhhhhhhhhhhh? This should warn users to call the sender beforehand.

**Should I trust an email that seems to come from someone I know?**

No, because this can be faked.

For example, examine the aforementioned Google Docs scam again. This phishing email was particularly effective because the scammers were able to infiltrate everyone's contact list and then spoof those contacts in the To field of an email.

**How do phishing attacks spread so quickly?**

They spread mainly because of how quickly some Internet users click links in their emails, without exercising any caution.

**How did "phishing" get its name?**

Scammers "fish" for sensitive data by dangling e-mail lures in front of Internet users. Most users won't bite the lure, but enough of them do to make the practice worthwhile for scammers and a nuisance to others.

Spelling the word "phishing" with a ϕ is a nod to phone phreaking, the first major method of computer hacking.

**Do phishing attacks occur only via email?**

No, phishing attacks do not occur only via email. Generally speaking, phishing is an attempt to get someone to unwittingly provide their sensitive data to an untrustworthy source. If we include this broad definition, then there are a number of other ways for phishing attacks to occur:

- Instant messages (or IM)
- Cell phone text (SMS) messages
- Chat rooms
- Fake banner ads
- Message boards and mailing lists
- Fake job search sites and job offers
- Fake browser toolbars

**Do all phishing attacks target random Internet users?**

No, not all phishing attacks target random people. **Spear phishing** occurs when scammers target specific users by researching their social media profiles, then sending detail-rich emails to their targets. Internet users are more likely to trust emails when they contain specific details about themselves.
These spear phishing attacks may even become more prevalent with the 2017 Equifax hack.

**ITS Help Desk**

(850) 474-2075  
helpdesk@uwf.edu