10 Ways to Fight Phishing

Phishing emails—fraudulent messages that try to trick you into providing passwords or personal info—are among the most common IT security threats.

But phishing attacks only work if we let them. Here are 10 things University of Iowa students, faculty, and staff can do to stop phishers cold.

Protect your info.

Never provide personal, financial, or account information in response to an email, message, or phone call. Legitimate organizations don't ask.

Ignore 'urgent' demands.

Claims that something bad will happen if you don't act right away are almost always phony. Don't fall for them.

Check every link.

Hover your cursor over links (or press and hold on mobile devices) to see where they really go.

Learn to read URLs.

Website addresses (or URLs) follow certain conventions. Look for appropriate domain extensions like ***.com, .edu, or .gov.***

Type instead of clicking.

Rather than clicking links in emails, type website addresses directly into your web browser.

Make sure websites are secure.

Safe sites use secure connections—look for ***https://*** in their URLs. The s stands for secure.

Spot spelling and grammar goofs.

Phishing messages often include errors you don't see in legitimate messages.

Report phishing attempts.

If you receive a suspicious email, send it to ***ui-phishing@uiowa.edu***

Follow up on legitimate alerts.

If the ITS Help Desk alerts you about an account breach, contact us and reference the ticket number provided.

When in doubt, delete.

If an email feels like phishing, it probably is. Trust your instincts.

For an overview of anti-phishing tips, see: ***its.uiowa.edu/phishing-tips***
For reporting instructions, see: ***its.uiowa.edu/report***

If you think you've been a victim of phishing, contact the ITS Help Desk:
Phone: ***319-384-4357 (4-HELP on campus phones)*** | Email: ***its-helpdesk@uiowa.edu*** | Live chat: ***helpdesk.its.uiowa.edu/connect***

#FightPhishingUI

THE UNIVERSITY OF IOWA its **INFORMATION TECHNOLOGY SERVICES**