TIPS TO AVOID PHISHING SCAMS

WHAT IS PHISHING?

"Phishing" is the use of fraudulent email, websites, text messages and phone calls to trick people into disclosing personal financial or identity information, such as credit card or Social Security numbers, user names (e.g., NetID) and passwords.

This brochure provides tips to identify and avoid phishing scams and to evaluate whether a University email containing a request and/or links is legitimate. If your group or department sends mass emails, this brochure can help you make sure they do not appear as phishing attempts.

REPORT PHISHING OR SPAM

- To report phishing emails that appear to be from within the UW-Madison campus, email **abuse@wisc.edu**.
- To report emails that appear to be spam, forward the email to **is-spam@doit.wisc.edu**.
- To report general phishing emails, go to **antiphishing.org**.

HOW TO RECOGNIZE SCAMS

Scam tactics are increasingly sophisticated and change rapidly. Even if a request looks genuine, be skeptical and look for these warning flags:

- The message is unsolicited and asks you to update, confirm or reveal personal identity information (e.g., full SSN, account numbers, NetID, passwords, protected health information).
- The message creates a sense of urgency.
- The email is not digitally signed.
- The message has an unusual “From” or “Reply-To” address instead of a “@wisc.edu” address.
- The (malicious) website URL doesn’t match the name of the institution that it allegedly represents.
- The website doesn’t have an “s” after “http//,” indicating it is not a secure site.
- The message contains grammatical and/or spelling errors.

As a rule, UW-Madison **WON’T** ask you to disclose **PERSONAL** identity **INFORMATION** via email.

DO'S AND DON'TS

✔ **Do** keep your Internet browser and operating system up to date with the latest security patches and updates.

✔ **Do** look for a digital signature or certificate as another level of assurance that senders are who they say they are. Digitally signed messages will appear with a red ribbon on the far right side and will also state that it has been digitally signed by the sender. To request a digital signature for an individual or department, visit **go.wisc.edu/digital-signature**.

✔ **Do** validate that you are connected to a certified, encrypted website. Look for a closed padlock in the URL address line or the status bar at the bottom of your browser window, for "https:" rather than "http:" in the URL, and a green address bar that confirms the site has been verified as authentic. Also, click the logo in the URL address line to view details about the site's encryption certificate (if one is present).

✔ **Do** use common sense. If you have any doubts, don't respond. Contact your department IT representative or the DoIT Help Desk at **(608) 264-HELP (4357)** for advice.

✖ **Don't** click the link. Instead, phone the company or do an Internet search to confirm the company's true web address.

✖ **Don't** use forms that are embedded in the body of an email, even if the form appears legitimate.

TIPS FOR SENDING MASS EMAILS AT UW–MADISON

The following tips can help departments create mass email messages that won't be perceived as phishing attempts:

- Don't ask for personal identity or financial information in an email.
- Always send from a wisc.edu address and use a wisc.edu reply-to.
- Use a digital signature. (See "Do's and Don'ts" section)
- Avoid sending web links whenever possible, especially non-wisc.edu links. Scammers use seemingly legitimate links to install malware.
- Avoid sending attachments. They are frequently used to spread viruses or install malware.
- Consider working with the My UW-Madison team to host your content or application in the campus Portal. Users must present their credentials to access this secure environment.
- Within the email body, encourage recipients to contact your department or the DoIT Help Desk to verify the email is legitimate before they respond.

Get more info at **kb.wisc.edu**, **article #52781**

Q&A

What is personal identity information?

Information that can be used to uniquely identify, contact or locate a single person. Personal information includes, but is not limited to, Social Security, driver's license and financial account numbers; user names and passwords; street and email addresses; telephone numbers; or biometric data (e.g., fingerprints, DNA).

Is it okay to give out personal identity information to the University via email?

No. Because it can be very difficult for recipients to identify counterfeit emails, UW-Madison won't, as a rule, ask you to disclose personal identity information via email. Scammers will sometimes pose as "the University email service" or "the campus tech support service." Don't be fooled! If you are asked to disclose your identity information, don't do it. When in doubt, contact your local IT professional or the DoIT Help Desk at **(608) 264-HELP (4357)** or visit **helpdesk.wisc.edu**.

What happens if I do respond to a phishing attempt?

If the University logs any response by you to a known phishing address, your credentials (i.e., NetID and password) will be disabled and you will not be able to access network resources until you re-establish your University identity credentials.

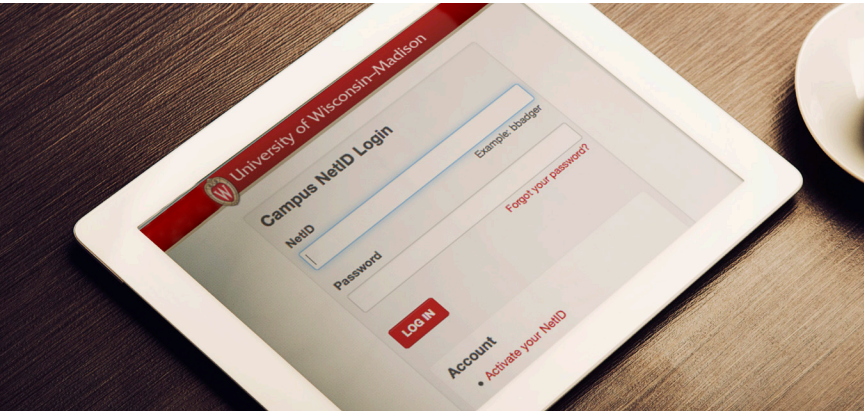
Is exposure of my NetID and password really that risky?

Yes. Someone can use your NetID and password to access your personal information in the My UW Portal, including your payroll statements, financial aid records, grades, home address and more. With your NetID, someone can steal your identity, change your course schedule, alter your research, and gain access to applications within your department or even your home computer.

Will UW–Madison ask me for personal identity information by email?

The Office of Cybersecurity discourages campus groups from sending these types of requests; however, there may be necessary exceptions (e.g., IRS Form 1098T requests). If a unit does have a legitimate need for requesting personal identity information (e.g., a Social Security number) via email, follow these guidelines:

- Alert users that an email requesting sensitive data is forthcoming (e.g., via a low-threat email with no links, department newsletter or website, or campus publication).
- Notify key campus stakeholders, such as the DoIT Help Desk or the Office of Cybersecurity, that such an email is being sent.
- Encourage users to call the department directly or the DoIT Help Desk if they question the legitimacy of the request.



Office of Cybersecurity

CIO AND VICE PROVOST FOR INFORMATION TECHNOLOGY

UNIVERSITY OF WISCONSIN–MADISON

OFFICE OF CYBERSECURITY

go.wisc.edu/cybersecurity | cybersecurity@cio.wisc.edu

GET FREE HELP

it.wisc.edu/help