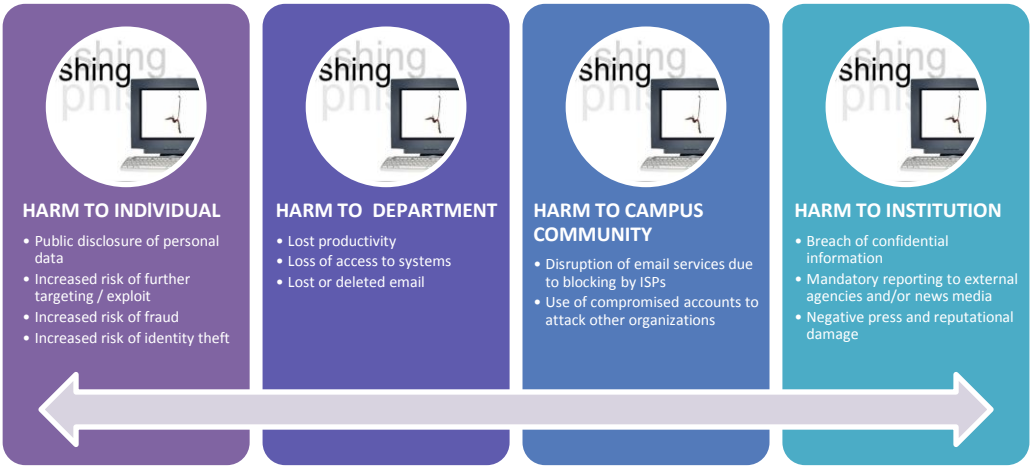
Protect Yourself From Phishing

Malicious email is a universal problem, but poses a special risk for users with access to sensitive data. Phishing messages frequently contain links to malware that can compromise workstations, and can often trick users into divulging passwords that could provide an attacker with access to sensitive information.

The impact of phishing ranges from the individual all the way to the institution. The following chart illustrates the harm caused by phishing:



UW Whitewater's Training Program

To help campus users understand how to recognize malicious emails and to assist the University in managing the associated risk, ICIT has created a series of D2L training modules covering the following information security topics:

- General awareness and Internet Safety
- Student records security
- Financial records security
- Protecting yourself and your family at home
- Criminal records security
- Credit card data security
- Health records security

Employees with access to sensitive information are required to complete this training.

How do employees access the training?

Employees self-register for the training by logging into D2L at https://d2l.uww.edu and selecting "Self-Registration" from the Tools menu in the upper right corner of the screen:

The course name is OTHER-MISC-Information Security Awareness. Once the employee has self-registered, it will appear in the user's course list and can be accessed at login.

Questions?

If you have problems access the D2L course, please contact UW-Whitewater's D2L support team by submitting a D2L support form at https://www.uww.edu/desire2learn/contact-d2l-support and indicate that you cannot log in to D2L in order to take the ICIT Security Training course.
If you have questions, comments or feedback about the security training or our security awareness efforts, please contact security@uww.edu.

UNIVERSITY OF WISCONSIN WHITEWATER | ICIT