How to Protect Yourself From Common Scams

- If you get an email or pop-up message that asks for personal or financial information, do not reply.
- The IT department will NEVER ask you to verify your password in an email so do not verify in an email.
- WSU laptops already have Antivirus software DO NOT install another antivirus software.
- You have not won the lottery in Spain, the Netherlands, Canada or anywhere else. You didn’t buy a ticket, did you? Do not reply to these emails.
- A poor widow or bank manager does not need your help to move money from a dead person’s account to another place so do not reply.
- The IRS is not electronically auditing you so do not reply.
- The jury duty clerk never calls for your Social Security number so do not provide it.
- Banks and credit card companies do not email you to verify your account information so do NOT reply.

WSU Technical Support Center HOURS

Winona Main Campus - Walk-In Support
Somsen Hall 207
Monday - Thursday: 7:30 am - 8:00 pm
Friday: 7:30 am - 4:30 pm
Sunday: 2:00 pm - 7:00 pm

Winona Main Campus - Walk-In Support
Lourdes Hall, G-46
Monday - Thursday: 1:30 pm - 9:30 pm
Friday: Noon - 4:00 pm
Sunday: 2:00 pm - 9:30 pm

Rochester Campus
Monday - Thursday: 8:00 am - 9:00 pm
Friday: 8:00 am - 4:30 pm

Summer Hours
Somsen Hall, 207
Monday - Friday: 7:30 am - 4:30 pm
Lourdes Hall, G-46
Closed for the summer
Rochester Campus
Monday - Friday: 7:30 am - 4:30 pm

Information is also available on the WSU Technology Knowledge Base (wiki) or http://www.winona.edu/it for future reference.

Winona State University
IT Department

Phishing/Private Data Protection

IMPORTANT!
Please Read Carefully

TSC Phone Support
507.457.5240
What is Phishing?

PHISHING IS SERIOUS BUSINESS! IT THREATENS YOUR SECURITY ALONG WITH THE SECURITY OF WINONA STATE UNIVERSITY.

Wikipedia’s definition of phishing: “Phishing is the act of attempting to acquire sensitive information such as usernames, passwords, and credit card details (and sometimes, indirectly, money) by masquerading as a trustworthy entity in an electronic communication.”

The most common form of phishing is emails pretending to be from a legitimate retailer, bank, organization, or government agency. The sender asks to “confirm” your personal information for some made-up reason: your account is about to be closed, an order for something has been placed in your name, or your information has been lost because of a computer problem. Here at Winona State they may make it sound like the IT Department wants you to confirm your username and password. THE WSU IT DEPARTMENT WILL NEVER ASK YOU TO REVEAL PRIVATE INFORMATION IN AN EMAIL.

Questions?

If you have any questions please contact TSC Phone Support at 507.457.5240.

What Should You Do?

- If you receive an email that asks for your PASSWORD, CREDIT CARD, or any other private data - **DO NOT respond** (email, web form, etc.). Although these emails can (and usually do) look official and appear to be sent from a legitimate source, they are **SCAMS**. The WSU Information Technology Department will **never ask you** to reveal private information such as your password via email. This is also true of your Bank, PayPal, eBay, etc.
- The safest way to protect yourself is to **NEVER share your password(s) with anyone**.
- Don’t click on links within emails that ask for your personal information.
- Never enter your personal information in a pop-up screen.
- **Report Phishing Emails**
  - To help the WSU IT Department identify security threats please forward any emails that ask for your password to abuse@winona.edu.
  - **If you suspect or know that private data is being used or shared inappropriately, refer to the Minnesota State system Breach Notification Standard** and contact your supervisor or the IT Department.

When to Protect Private Data

- Any private data stored on laptop computers, transmitted across the Internet, or transmitted using wireless technology must be protected.
- Extra precautions should be taken with Social Security Numbers and credit card information because of identity theft concerns. Encryption or other secure transmission is required when handling Social Security Numbers in electronic form.

Examples of Private/Non-Public Information

- Social Security Numbers
- Credit card information
- Trade secret or intellectual property
- Individual demographics such as:
  - Age, race, ethnicity, gender, citizenship, visa status, veteran or disability status;
  - Employee home address/phone; dependent information;
- Personal medical information
- Library use information
- Parking lease information
- Student grades, courses, class schedule; student worker information
- Student discipline, educational services received, test scores, admissions, financial aid records
- Employee performance evaluations

Portions of information contained in this brochure are taken from the MNSCU D2L training modules—Public Jobs: Private Data