Password Security

- Avoid the ‘save’ my password option on websites
- Never use your UMass Lowell credentials on non-university applications (i.e. Facebook)
- If it’s in the dictionary or someone’s name—it’s a bad password. Use special characters, numbers, and upper/lower case
- Never share your UMass Lowell password with anyone
- Don’t use the same password for all systems
- Remember: Information Technology will NEVER ask you for your password via email.

REPORTING A SECURITY BREACH

Act Immediately

Breaches are a serious matter and must be handled following a strict protocol. The University is required by Massachusetts state law to report data security breaches immediately.

If you know or suspect a breach has occurred involving sensitive information, contact the Information Security Office as soon as possible to coordinate incident management.

Information Security will help you:

- Identify and contain the breach
- Understand the laws and regulations
- Assist you in adjusting your procedures to avoid future issues

Do We Have A Policy For That?

Policies Are Important!

- Information Security Policy
- Acceptable Use Policy
- Email Usage Policy
- Encryption Policy
- Data Classification Policy
- Mobile Device Policy
- Wireless Policy

Visit www.uml.edu/IT/Polices for more information on polices and standards

Visit www.uml.edu/IT/Information-Security for more information on information security at UMass Lowell.

University of Massachusetts Lowell

Information Security
University Crossing, Suite M50
220 Pawtucket Street
Lowell, MA 01854

infosec@uml.edu  (978) 934-4357
www.uml.edu/IT/Information-Security
Get Anti-Virus Protection: Protecting your devices from viruses is a full time job. Go to the University’s IT website to get the latest AV software for your Windows or Mac devices. Visit www.uml.edu/software

Look for the ‘s’ in https: In today’s world, “spoofing”, or making a malicious webpage look like the real thing, is all too common. The ‘s’ in https means your connection is encrypted. Fake websites typically do not encrypt their connections. Pay close attention to your browser warnings when it’s telling you’re visiting a non-secure or malicious website. Never put a username or password into a web page that does not have the ‘s’ in https.

Think Before You Click: If you’re asked for your personal information (name, address, password, etc.), take a closer look before proceeding. Are words misspelled? Is the URL slightly off? Chances are you are on a malicious site. Just because the logos are real doesn’t mean the website is legitimate. STOP. THINK. CONNECT.

Don’t Get Hooked: Phishing emails continue to be a serious threat to the University. They target both your university credentials and personal information. Look for the following to spot phishing emails:
- Emotions: Greed, Urgency, Curiosity, Fear
- Fake Email Signatures, Sender Addresses, Email Tone
- Beware of: Attachments, Login Pages, Links

If you see something, say something. Report suspected phishing emails to the IT Service Desk (help@uml.edu) or the Information Security team (infosec@uml.edu).

Patches and Updates: Keeping your computer up-to-date with the latest patches is one of the best defense against hackers and the spread of viruses and Trojans. Make sure your computer is configured to update automatically. Don’t forget the applications too!

Back Up Important Files: No system is completely secure. It’s important to have your files backed up and stored in a safe place. Utilize secure network file shares when appropriate.

Protect Your Identity

- Before purchasing anything on the internet or providing any personal information (bank account, credit card, etc.) always make sure the webpage is secure. Look for the “https” in the web address. This tells you the transaction is encrypted.
- Standard email is not appropriate for sending sensitive or confidential information, as it is inherently insecure. Contact Information Security if you need to send an encrypted email for University business.
- Never collect credit card or bank account information via email. This violates University policy on accepting credit card information.
- Be careful sharing too much information on social media. Hackers are shifting their focus to target social media users. In less than 30 minutes, nearly anyone can learn your name, email address, location, past work experience, hobbies, and more just by looking at your profile.

Patch and Update

Be careful of storing restricted or sensitive information on your office computer, laptop, or portable media. Instead, store it on a secure network drive. However, if you must store this type of information on your computer or portable media for official business purposes, you must ENCRYPT it. Contact Information Security (infosec@uml.edu) for more information.