

Wireless Computing at UM-D

Wireless is Here !

Wireless computing is now a reality for faculty, staff, and students at UM-Dearborn! It offers most of the computing services that the wired network does, without the restraints of a network cable and jack. After getting connected, you can use your laptop to login to University systems, check email, and surf the Internet.

DO YOU KNOW YOUR UNIQUAME & DEARBORN PASSWORD?

Everyone at University of Michigan is assigned a **uniquame** – a personal identifier for all computing access and logins.

Your **Dearborn password** is needed to login to the wireless network. It's the same one used to access campus email.

If you don't know your unquame or Dearborn password, visit the ITS Accounts Office located in 1141 CW. You can also contact them at (313) 593-3274 or accounts@umd.umich.edu.

You Need to Login

For security purposes, UM-D's wireless network is only available to campus users. To access it, you will need to login.

Logging in is fast and simple !!

- When you turn on your wireless laptop and open an Internet browser, you will be directed to UM-D's wireless login screen.
- Enter your Uniquame and DEARBORN password.
- Your browser will return to your web page.

Your session will remain open until your laptop is inactive for an extended period or you "roam" out of range. If this happens, just login again to the wireless network.

It is important to remember that the wireless network is a shared resource, intended to supplement the campus wired infrastructure – not replace it.

Security! Security! Security!

Security is a major issue with wireless networks. Take precautions and use care in handling data.

- Install a personal firewall on your laptop. (Windows XP and Vista have a built-in firewall. Or you can download freeware, such as *ZoneAlarm*.)
- Install anti-virus software. University of Michigan offers free McAfee *VirusScan* software. Be sure to update it regularly and run frequent scans on your laptop.

Since signals are passed through the air, wireless transmissions can be intercepted, and data can be viewed in clear text (including passwords). ***The built-in wireless LAN security is known to be flawed, and should not be relied upon to protect privacy.*** If you are concerned about the privacy of information being transmitted by wireless, you should take steps to encrypt it (using Secure Sockets Layer or SSL, SSH, etc). UM-Dearborn members needing enhanced security can utilize Virtual Private Network (VPN) technology.

WEB RESOURCES

UM-D's Wireless Login: <http://login.wireless.umd.umich.edu>
UM-D's Wireless Policies: <http://www.its.umd.umich.edu/106>
UM's Anti-Virus Software: <https://webapps.umd.umich.edu/itslabs/itsDownloads>
UM-D's VPN Instructions: <http://www.its.umd.umich.edu/7115>
ZoneAlarm Downloads: <http://www.zonelabs.com/store/content/home.jsp>