Introductory Security Video

Basics of Security at the Law School

Law School students taking a clinic during the course of their education may handle sensitive attorney-client data, and have a legal and ethical obligation to take the necessary precautions to protect that data from exposure.

Your clinical faculty will provide more details, but the following list provides a minimal set of requirements

- **Secure your personal device**
  This includes wireless routers, mobile devices, and Internet of Things devices. Each link in the internet environment is important to protect. The more thorough you are, the less likely your systems will be compromised.

- **Remove sensitive data from your personal device**
  You may already have sensitive personal data on your device. It is advisable to remove everything possible. Never store University data on your devices.

- Only store clinic data in the U-M Box folders assigned to your clinic – never on your personal Box space. The folder name will begin with “UMLS -”.

- For clinic work, use the clinic’s group email, never your own. And never use a non-university email account, which lacks the security assurances provided to the University by Google Mail.

Current Security Issues seen at the Law School

- **Phishing and Suspicious email**
  Common types of phishing seen at the Law School include tax fraud, impersonation of University/Law School officers or faculty, and purported email system errors. Included on this page are instructions for reporting phishing email to the University’s security group.

- **Scams and Fraud**
  Tech support scams, both electronically and on your phone, lead the list of scams, but this category also includes recent COVID-19 scams offering research jobs to UM students, and tax collection scams, among others.

- **Ransomware**
  Keeping your system updated will reduce the ability of ransomware to use operating system and application vulnerabilities to infect your system and encrypt your data. Ransomware is also a particularly good reason to store copies of all your important electronic documents in a remote, disconnected location.

- How to spot a [misleading sender address](#)
Being able to spot misleading headers reduces the possibility your device will be compromised by any of the above issues. It only takes a moment, once you know the signs, to react proactively and prevent data loss or identity theft.

Contacting Law School Information Technology staff for help

- LawITStudentSupport@umich.edu