Keeping UMass Cyber Safe

TIPS FOR WORK & HOME

**PASSWORD SECURITY**
Use two-factor authentication when available to ensure that only you can access your account.

Use passwords with a mix of numbers, upper/lower case letters, and at least 10 characters.

Never use your work passwords for personal logins.

**EMAIL AND WEB SAFETY**
You are a target to hackers so be careful what you click.

If it sounds too good to be true, it probably is!

Don’t trust email from people you don’t know.

If your anti-virus warns you, believe it!

**CONNECTIVITY**
Don’t broadcast Bluetooth and/or Airdrop information; it’s an open invitation for hackers to attack your devices.

Be cautious when using public Wi-Fi, and use your phone as a mobile hotspot or connect via VPN whenever possible.

**DEVICE SECURITY**
Always lock your computer when leaving it unattended; don’t just wait for the screensaver to automatically lock the screen.

Don’t leave your laptop or phone unattended in public.

**PROTECTING YOUR INFORMATION**
Safeguard personal identifiable information online and off. (Remember to shred!)

Don’t trust public computers ever!

Backup your data.

**SHARING**
Use UMass authorized storage options such as Dropbox, for securely storing and sharing files.

Do not share passwords or accounts requiring login.
ACCESS AND SECURITY
We log all access to our applications and run those applications in a secure manner.
We protect our data and applications using DUO multi-factor authentication to confirm your identity when logging into UMass systems.

DEVICE SECURITY
We automatically encrypt hard-drive data on your UMass-issued computer.
We install and provide Sophos Anti-Virus to protect you both at work and for home use.

EMAIL SAFETY
We scan all emails for malicious attachments and block them from your Inbox when discovered.
We protect you from email phishing exploits and provide a way to report potential phishing attempts.
(No system is infallible, we rely on you to help monitor potential email threats.)

PROTECTING YOUR INFORMATION
We protect the UMass datacenter with firewalls, intrusion detection, and physical access security.
We use multiple types of security measures, each protecting against a different type of threat.
We provide secure ways to dispose of paper documents.

PROTECTING YOU 24 x 7 x 365
We provide training to all employees to help make us more secure.
We undergo continual third-party security assessments and seek continuous improvement.
We protect the UMass brand.

Questions? We’re here to help!
helpdesk@umassp.edu or 774-455-7777

University Information Technology Services

REV 012420