

CYBER SECURITY

is essential to the mission of Iowa State University. We have a dedicated IT Security team that helps **safeguard the information and technology** used by the Cyclone community. Use these tips to stay more secure.



PROTECT YOUR NET-ID

Your Net-ID protects access to important university data. Help us **keep that data secure** by following these tips to protect access to your account:

- Use a long, hard-to-guess passphrase for your Net-ID password
- Don't reuse this password on another site
- Don't share it with anyone else
- Only enter it into login.iastate.edu
- ISU employees will never ask you for it
- If you receive an MFA push notification and you weren't logging in, choose "No, it's not me" and let security@iastate.edu know
- Don't send anyone your MFA text message code, even if they claim to be from ISU

GOOD CYBER HYGIENE



- Keep student and research data only on ISU computers and approved cloud services
- Set a screen lock on your computer and other devices
- Lock your computer when away
- Use full disk encryption to protect your data
- Use a password manager to help you remember all of your passwords
- Install official software updates quickly
- Only install software apps from official app stores or sites you trust
- Avoid fake software updates that lure you into installing malware—they always appear in a browser window

SPOT AND REPORT PHISHING

Watch out for common phishing emails:



Personal assistant job scams



Gift card scams



Fake invoice attachments

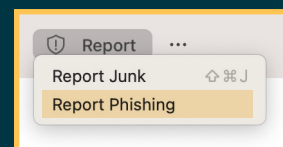


Links to web pages that look like login screens, but aren't ISU's



Links to forms that ask you to enter your password or other personal information

Report phishing emails using Outlook's Report button:



Learn more here:

