How to Avoid Getting Ransomware

Rich Tener
Chief Information Security Officer

security@iastate.edu
What is Ransomware?

- Type of malware that encrypts all your files
- It also sends a copy of your files to the attacker
- The attacker extorts you to decrypt/unlock them
- The attacker also extorts you to keep them private
- If an ISU employee gets ransomware and has access to student data, we could be handling a data breach
How does someone get ransomware?

- Password getting phished or stolen
- Installing malware
- Falling behind on installing security updates
Secure Your Accounts

• Hackers compromise sites and steal passwords
• They test those passwords against other online services
• Don’t reuse the same password on multiple sites
• Enable 2FA on your personal email account
• Sign up for haveibeenpwned.com to know when a site that you use has been breached
Don’t let your MFA get phished

• We require MFA for all employees
• MFA mitigates the risk of a password being stolen
• If you get an Okta push message and you didn’t log in to anything, say No, It’s Not Me
Use a Password Manager

- Creating unique passwords is difficult...
- Remembering passwords is difficult...
- Password managers can do both for you
- Remember one good password to unlock the vault
- The password manager handles pasting the correct password into each site
- LastPass, 1Password, KeePass, Dashlane
Install software from App Stores

- Free software is often bundled with advertising software (Adware)
- Use a trusted App Store instead:
  - Apple App Store
  - Microsoft Store
  - Software Center (ISU)
Install software updates

- MacOS System Preferences, App Store, and Windows Update will tell you when you need to install updates
- Install them quickly!
- Some apps may also use native MacOS and Windows notifications to inform you about updates
Watch out for fake software updates

- They’ll lure you to install malware
- They always appear in a browser window
Unsolicited Microsoft Word docs

• Embedded macros will hack you
• You can safely preview these in Outlook Web
• Don’t enable content or editing
Look for phishing attacks

• They can come through email or other messaging apps
• Click links, but be mindful of what happens next
• If you end up somewhere unexpected or are asked to do something unexpected, let us know
• Inspect the sender email address

-----Original Message-----
From: Wendy Wintersteen <officep31@gmail.com>
Sent: Friday, July 19, 2019 1:20 PM
To: [Redacted]
Subject: Availability Request

I'll need you to complete a task for me discreetly, let me know if you are available.

Regards,
Wendy

• Don’t buy gift cards without calling the requestor first
• Don’t enter your password into a non-iastate.edu site
• Forward suspect emails to security@iastate.edu
Backup your data to a cloud service

- Protects you against ransomware
- Protects you against a storage failure
- Google Backup and Sync is free for Windows / MacOS
- OneDrive backs up important folders on Windows
QUESTIONS?