Ransomware Protection Checklist

Layered defenses to prevent ransomware from holding your data hostage

21 items • nexusitnm.com

BACKUPS

- [ ] Follow the 3-2-1 rule: three copies of your data, on two different media types, with one stored offsite.
- [ ] Use an automated backup solution so backups run without manual intervention.
- [ ] Store at least one backup offline or in a cloud service that is not mapped as a network drive.
- [ ] Ransomware often targets mapped network drives and cloud sync folders -- verify your backup is protected.
- [ ] Test your backups by actually restoring files from them. An untested backup is not a reliable backup.
- [ ] Verify your most recent backup ran successfully at least once a week.

PATCHING AND SOFTWARE

- [ ] Enable automatic updates for your operating system.
- [ ] Keep all applications updated, particularly web browsers and email clients.
- [ ] Remove software you do not use -- every unused application is a potential vulnerability.
- [ ] Keep your router and any network-connected devices on current firmware.

EMAIL AND PHISHING

- [ ] Be skeptical of unsolicited emails with attachments, even from people you know.
- [ ] Do not enable macros in Office documents received via email unless you are certain of their source.
- [ ] Hover over links in email before clicking to verify the actual destination URL.
- [ ] Report phishing emails rather than just deleting them -- it helps protect others.
- [ ] Enable your email provider's spam filtering and anti-phishing features.

ENDPOINT AND NETWORK

- [ ] Install reputable endpoint security software and keep it updated.
- [ ] Enable your operating system's built-in ransomware protection features.
- [ ] Limit user account privileges -- do not use an administrator account for daily tasks.
- [ ] Disable remote desktop access if you do not actively use it.
- [ ] Use multi-factor authentication on any remote access solutions.
- [ ] Segment your network so a compromised device cannot reach all other devices.

> This checklist is provided for informational purposes by Nexus IT Services, LLC. It is not a substitute for a professional security assessment. Contact us at (575) 263-6855 or nexusitnm.com if you need help implementing any of these items.