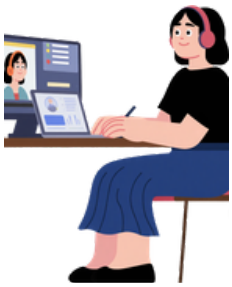
HOW TO PROTECT AGAINST RANSOMWARE

IN FOUR EASY STEPS



1

USER EDUCATION

The most common way ransomware attackers gain access to your systems is by being allowed entry by unwitting employees. Ensure your staff is aware that clicking a link, entering information on a fake page, or opening a file can expose your company to risk.

PATCH YOUR SYSTEMS

End-user machines and critical production systems should be patched regularly. Patching can be a tedious process that requires consistency, compliance, and proactivity. While patching can be done manually for smaller organizations, I recommend investing in a tool.

2

3

INVENTORY WHAT YOU HAVE

Many organizations are unaware of vulnerabilities because they lack a complete inventory of the software their users use. This is particularly true in SMB shops that have not locked down their environments, thereby granting users full local administrative privileges.

HAVE IMMUTABLE BACKUPS

Ransomware attackers know that one of the best ways to defeat a ransomware attack is to restore critical data from backup. Backups are now routinely targeted in ransomware attacks. To ensure your backups are safe, run a nightly backup in Write-Once, Read-Many (WORM) format.

4

LEARN MORE

Allow me to walk you through these steps, assess your organizational readiness and risk profile, and implement a comprehensive plan to protect your organization. For more information, visit my website: https://www.itladvisory.com