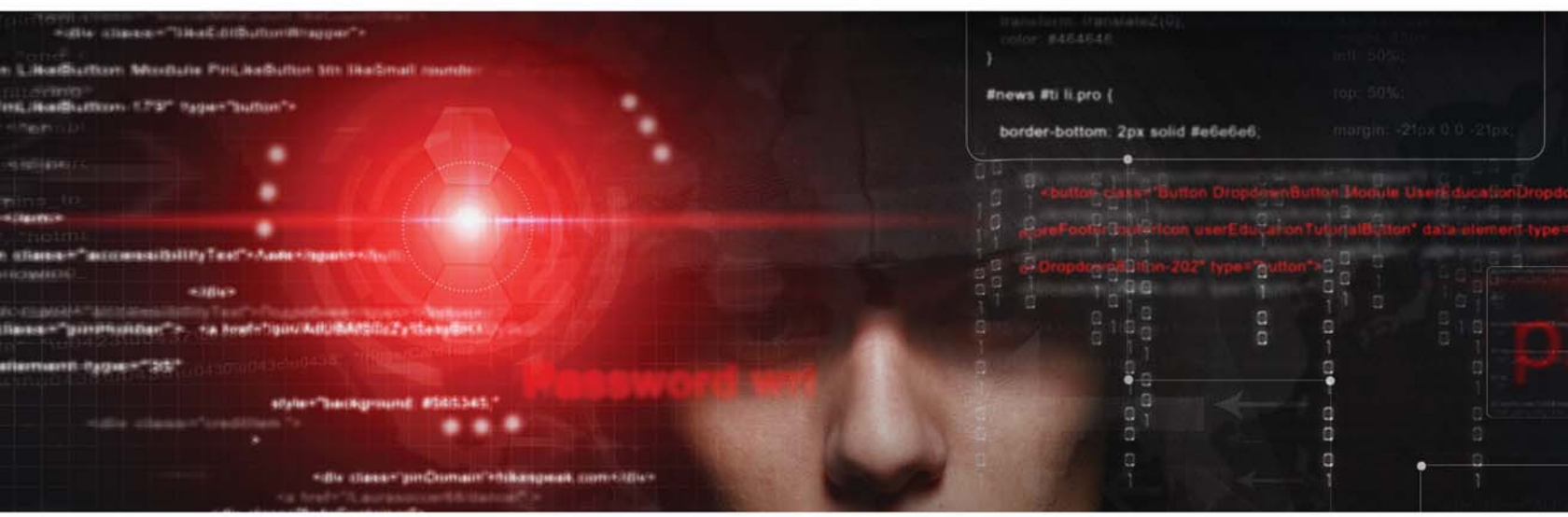
The Fundamentals for **Protection Against Ransomware**

Cybercrime is an ever-present threat to modern businesses, regardless of the industry. Without up-to-date and varied security measures, malware and successful hacks can compromise your customers' and employees' sensitive data and harm your systems, resulting in costly downtime and liability.

If you think that your business won't attract hackers, think again. Cybercriminals target smaller businesses specifically because of their apparent lack of IT security measures.

Small to medium-sized businesses like yours need to think past the size of their organization and realize that everyone is at risk for cyber-attacks. Without the right knowledge, tools and technology to prevent hackers from stealing your information, your business is left prone to a major data breach.

A recently popular type of malware is the "ransomware" variety, which encrypts a victim's files (making them unreadable) and only offers the key to recover them after a ransom has been paid. The unfortunate reality is that when it comes to your business' vulnerability to ransomware and other types of malware, it's not a matter of IF, it's a matter of WHEN. There are simply too many varieties of ransomware to guarantee total safety for your business.



Tier One Technology Partners
11311 McCormick Road, Suite 100 · Hunt Valley, MD 21031
70 Thomas Johnson Drive, Suite 100 · Frederick, MD 21702
www.tieroneit.com · Phone: (443) 589-1150 · Toll Free: (800) 431-2282

tier one
TECHNOLOGY PARTNERS
A division of MKS&H

Protection Against Ransomware

IT security can be a complicated and scary subject when it comes to modern cybercrime tactics such as ransomware. Most business owners cannot confidently claim that their business's network is secure. Can you?

Not sure where to begin? Follow these Fundamentals for Protection from Ransomware:

- **Stop hackers at the door:**
  Your first step is to protect your network with a firewall and antimalware solution from an industry-standard provider. While a no-name or off-brand vendor may cost less, security is really the one thing that you don't want to cut corners on.

- **Update your software:**
  Never ignore software update and patch notifications. Software updates are not only meant to improve the functionality of software; they also serve as a patch for recently identified vulnerabilities that can be exploited by hackers.

- **Educate End-Users:**
  A successful ransomware attack almost always relies on the participation of an unknowing user. Be sure that all staff members know how to recognize a ransomware scheme, and to avoid downloading and opening unknown email attachments.

- **Enable Windows Policies:**
  By blocking access to Volume Shadow Copy Service (VSS), you can stop certain types of ransomware from erasing your file backups.

- **Disable Script Hosting:**
  By disabling the Windows Script Host engine that allows VBS script files to run, you remove a key part of ransomware methodology that cybercriminals use to either cause a disruption or download a more advanced and dangerous malware onto your system.

Tier One Technology Partners
11311 McCormick Road, Suite 100 · Hunt Valley, MD 21031
70 Thomas Johnson Drive, Suite 100 · Frederick, MD 21702
www.tieroneit.com · Phone: (443) 589-1150 · Toll Free: (800) 431-2282

tier one
TECHNOLOGY PARTNERS
A division of MKS&H

Protection Against Ransomware

- **Employ an Email Filter:**
  Given that ransomware often enters a system as an email attachment, it's vital to filter .EXE files from incoming messages.

- **Backup:**
  The best contingency for a successful ransomware attack is a comprehensive, reliable backup. Whereas every other tactic is preventative, backups are often the only hope once ransomware has gotten into an IT environment.

- **Stay up to date:**
  As with all modern forms of cybercrime, in order to ensure your protection, you have to stay up to date on the latest developments in ransomware tactics. Cybercriminals will continuously innovate and improve the ways they attack, so don't let you and your business fall behind.

Yes, that's a lot to handle in addition to the day in and day out management of your business, but the good news is that you don't have to handle IT security on your own.

Tier One Technology Partners
11311 McCormick Road, Suite 100 · Hunt Valley, MD 21031
70 Thomas Johnson Drive, Suite 100 · Frederick, MD 21702
www.tieroneit.com · Phone: (443) 589-1150 · Toll Free: (800) 431-2282

tier one
TECHNOLOGY PARTNERS
A division of MKS&H

Protection Against Ransomware

As vital as each one of those tasks are for your security, there is still the problem of making sure they are all done on a regular basis. That's where a trusted partner in IT support can be so helpful. By having an expert team of IT security professionals assess your network and manage its many aspects, you can ensure that your technology is secure, without having to see to it yourself.

Tier One Technology Partners protects your business from Ransomeware and malware.

The Tier One Technology Partners team of IT security professionals understands that many businesses like yours are often unknowingly operating on outdated security models. Our team will assess your entire environment to identify any opportunities for improvement so that you can be sure you're in a better position to be protected from ransomware and other types of malware.

Don't let an outdated security culture leave your business vulnerable! Get in touch with Tier One Technology Partners at (443) 589-1150 or info@tieroneit.com to start fighting back against ransomware immediately.

Tier One Technology Partners
11311 McCormick Road, Suite 100 · Hunt Valley, MD 21031
70 Thomas Johnson Drive, Suite 100 · Frederick, MD 21702
www.tieroneit.com · Phone: (443) 589-1150 · Toll Free: (800) 431-2282

tier one
TECHNOLOGY PARTNERS
A division of MKS&H