WHITEPAPER

PROTECT FROM RANSOMWARE ATTACKS IN 10 STEPS

2025

NPC DataGuard™

SECURE MANAGED COMPUTING™

Reading Time: 10 minutes

Introduction

Ransomware has become a second pandemic affecting businesses of all sizes, from the one-person office to multinational corporations. Direct and collateral damage costs are now in the billions annually. Prevention is by far the best strategy to avoid the cost and reputational damage of an attack. This brief whitepaper will outline the 10 most important defense strategies and techniques to protect your business in a convenient checklist format — from NPC DataGuard, the leader in Secure Managed Computing™.

If you think you're too small to be hit by ransomware, think again. Companies of every size are vulnerable. Cyber criminals do not care who they hurt — they only want to extract as much money as possible from their victims. Just check the news to see proof of this; ransomware has even shut down healthcare systems and utilities, putting lives at risk. While the media focuses on the big events, it is critical to know that damage from ransomware to a 10-person professional services office is common, and can be even more destructive to that business than to a well-heeled multinational.

What is ransomware and what is the problem?

A ransomware attack occurs when a software virus penetrates a computer or computer systems, often through a single user's device when they click on an infected email or website link. This virus, also called malware, uses powerful encryption (scrambling data against a password key) to lock up the affected computer's information and that of connected systems. Only the attackers have the key to unlock the encrypted information. They may also download some or all the information from the affected systems.

The attackers then demand a ransom payment in exchange for the key to unlock the information or systems, or to prevent publication of what may have been stolen. Various other threats can be made, including attacks on the victim's clients when client lists are stolen, as happened to patrons of a Finnish therapy firm[1]. That company went out of business as a result.

The consequences of an attack for a smaller business are huge. While a ransom demand can run into the tens of thousands or more, paying — which would not be recommended by law enforcement or your lawyer — can be the least of it. There is the cost of restoring systems, the cost of lost business, and the damage to your reputation. There are penalties for violation of contract terms or NDAs, and for infractions of securities laws or compliance violations, all of which can be expensive.

Overarching all is the risk that, even if you do pay, the criminals may not provide decryption keys — there is, as the saying goes, no honour among thieves. And there is also the risk that stolen data, even if the ransom was paid, has been retained for use in future blackmail with attackers demanding further payments.

According to the Sophos State of Ransomware 2024 report, which surveyed 5,000 IT/cybersecurity leaders across 14 countries, while on average 65% of data could be restored using the decryption key if it was supplied, only 8% of companies who capitulated and paid the ransom got all of their data back[2]. You also have no guarantee that your systems are not otherwise compromised, giving attackers a way in for future evildoing.

65% of data could be restored from paying ransom[2]

8% of companies were able to restore all data from paying ransom[2]

While no one can promise that you can be completely immune to ransomware — attackers are upping their game all the time — you can make it much harder for attacks to succeed by adopting these 10 strategies.

Regardless of whether you are undertaking this yourself, or just using it to cross-check what should already be in place in your business, make a realistic assessment of your current capabilities before you start. Decide, given the threat levels, if you have the skills and resources around you to protect your company or if you should rely on one of the new outsourcing models for security and support, such as a Managed Security Service Provider (MSSP). As the largest and most technically sophisticated companies in the world say, when it comes to cyber security, no one should go it alone.

You should also determine what you need to protect, and where an attack of this nature would be most devastating. That will also help you determine where to start.

And just a note if you are a business owner or non-technical leader: when this starts to get a little technical, don't tune out. It is essential that owners and leaders understand what is going on in their systems; maybe **not how**, but **what**. Most of these steps are at the least conceptually understandable, and they will allow you to ask the right questions of a current or future provider. Delegating "what is going on with us security-wise" to someone who has less skin in the game than you may leave you more exposed than you know.

So, here we go.

The 10 most important steps to protect from ransomware attacks

01 Enable multi-factor authentication (MFA)

We started with this one because many systems and services already have the capability. You just need to turn it on, so it will cost you nothing.

MFA is simply enabling an additional step such as entering a code sent to your phone when logging in to your email, a cloud service, your remote desktop, or VPN. Microsoft thinks a whopping 99.9% of cloud email account compromise attacks can be stopped by MFA[3].

With the shift to work-from-home, many small companies began to use remote desktop to connect to systems in the office, and weak authentication on a remote desktop or a VPN leads to breaches, which in turn allow the bad guys to plant ransomware in your computers.

Give some thought to what kind of MFA you use, especially if you are a high-value target like the owner of a professional services firm. Although rare, using SMS (text messages sent to your phone with an access code) can be breached through a SIM swap attack on your phone account. So, while it is secure, it is not quite as secure as an authenticator app, or push-based MFA that sends you a message asking you to approve access when you try to log in.

According to Microsoft, 99.9% of cloud email account compromise attacks can be stopped by MFA[3]

02 Set up your computers for security

Start at the beginning — the first thing to do when you get new computers is to set them up securely:

A. Choose computers for your business that are business-class. Some of the better models, like HP EliteBooks, come with excellent security tools. We are long past the time when a $600 consumer-grade computer with some basic anti-virus software can be the basis for protecting your business.

B. Don't assume because your computer is new that it's up-to-date (you can almost guarantee it isn't) — check for and apply all operating system (OS), application, and firmware (sometimes called BIOS) patches. Criminals exploit every weakness so make sure you get the basics right.

C. Do not accept default settings when setting up a computer's OS or applications — they favour the vendor's desire for information and ad revenue, not your privacy and security. And don't leave this to your tech or local provider; ensure you understand and are comfortable with what your applications are sharing about what you do.

   Pro Tip: Microsoft Edge, the new browser that ships with Microsoft Windows 11, has great privacy and security controls, with most of them enabled by default.

D. Choose applications for your computers that prioritize security. More and more, as a professional, you will get asked by clients, partners, and even new suppliers, what you do to secure the information they will share with you. Choose your applications and technology with security at the top of the list rather than price or slick marketing. Develop a checklist, or even a questionnaire to complete, that asks the right questions before you start entrusting a product to help run your business.

E. Create strong, unique passwords for your computers. Password length matters. For us at NPC, it starts at 14 characters. Or better yet, use *passphrases*, a string of unrelated but memorable words. If you

Setup your computers for security continued

find all of that too cumbersome, use biometric authentication (i.e. a fingerprint reader or facial recognition), that will enter a password with just a swipe. It will allow you to create long passwords that you may only ever type once when you add it to the biometric software. But, again, be sure you are using a business-class tool with an encrypted password manager; a password manager on your secure computer can keep all those passwords under control but be cautious about putting them in the cloud.

F. Change the default administrator password, and do not use an account with administrator privileges for routine tasks. If credentials are compromised, that gives attackers too much power. Employ the principle of least privilege on both personal machines and servers; only give a user the minimum permissions required to do their work. And if you are just doing regular work in the system yourself, use something less than the admin login.

G. Install appropriate anti-malware software and set it to automatically perform scans for malware. Use a business-class tool here. Spending $50 per year per user is one of the best investments you can make to protect your systems.

H. Enable your computer's encryption capability. BitLocker is a powerful encryption tool, but ensure you follow a careful process to protect the credentials and encryption certificate, or you could lock yourself out of your own data! If this sounds mystifying, get help from a professional.

Pro Tip: EFS (Encrypting File System by Microsoft) encrypts on a file-by-file basis, so using it in combination with BitLocker can hand the bad guys unreadable data in some scenarios when a breach was caused by another user's login.

I. Enable the personal firewall in your OS on your individual computers. Microsoft in particular has done a good job with their firewall technology in Windows 11, and it is on by default. On a Mac, it is off by default and needs to be enabled. In both cases, check it after you complete installing all your software to make sure it wasn't disabled. A personal firewall in addition to your network firewall or one your internet provider provides adds another layer of protection.

03 Patch your systems

Once you’ve set up secure computers, you can’t rest on your laurels. Keep all your other systems and programs patched as soon as new software updates become available. Make a list and make it a habit on a scheduled basis to ensure all critical and outward-facing systems are up-to-date. This must be policed and diligently managed. Put someone in charge of patch review, even a non-technical manager or administrator. If you have software so old it is not being patched and updated, it’s time to replace it.

04 Change all passwords

Change all passwords on systems, including those for hardware and applications, from time to time. Even that old Wi-Fi access point in the corner of the warehouse, and especially the one at home where you now mostly work can offer an attacker easy entry. And don’t use the same password on all devices and applications or reuse old ones. Here’s a primer on creating strong passwords: click here to watch video.

05 Disable macro scripts

A macro is a pre-programmed sequence of instructions that can be executed with a single keystroke or button click — a common tool used to automate repetitive tasks, but could be configured to download malware if you open a malicious file. Word, Excel, and other office software products should require a click to enable them to run, but disabling them will prevent any macros from being able to run without your express input.

06 Segment your network

If you have more than one server or a hybrid-cloud setup (a local server and cloud server talking to each other), segment as much as you can between the systems with different logins and passwords wherever possible. If you do get a malware penetration, this can limit the spread.

07 Back-up files regularly

Back-up files and ensure you do not stay connected to your backup location when not actively backing-up data. If you do, malware on your network could infect the backup as well. Test a restore from time to time to ensure the backup/restore process works.

08 Use a virtual private network (VPN)

Use a Virtual Private Network (VPN) when connecting to the internet or the office from locations outside the corporate firewall, even in your home. Other users on home networks could pass malware into your corporate network unless your connection is protected by a VPN.

09 Train, train, train

Teach your team how to recognize suspicious emails, texts, and instant messages. Remind them not to open unexpected attachments or click on links without verifying what's on the other side. Some malicious emails are extremely credible, so it's easy to be fooled; users should not feel embarrassed about checking carefully before clicking links or opening attachments, even if the message appears to be from their boss. Security is a team sport — make it an open dialogue. Create a culture where it's okay to be suspicious and stop the work for verification. No one should be afraid to ask questions, especially someone new to the team. It will keep everybody safer.

Users should all be trained not to open unexpected attachments or click on links without verifying where those links are taking them.

10 Have an incident response plan (IRP)

Have an Incident Response Plan (IRP) ready for the painful day if something sneaks past your preventative measures. Some say that it's a matter of when, not if — but at NPC we don't completely agree. Knowing what to do, what not to do, and whom to call can limit technical, regulatory, and brand damage. It can also keep you from ruining your chances for a speedy and less-costly recovery. So, to get you started, our gift to you — an IRP plan already laid out in a template format: click here to download.

Review - 10 Step Checklist

Protect From Ransomware Attacks in 10 Steps

01 Enable multi-factor authentication

02 Set up your computers for security

03 Patch your systems

04 Change all passwords

05 Disable macro scripts

06 Segment your network

07 Back-up files regularly

08 Use a virtual private network

09 Train, train, train

10 Have an incident response plan

Additional Resources

- Canadian Centre for Cyber Security | Government of Canada
- New cybercrime and fraud reporting system | Royal Canadian Mounted Police
- The U.S. Cybersecurity and Infrastructure Security Agency | The United States Government
- FBI Internet Crime Complaint Center (IC3) | Federal Bureau of Investigation
- The No More Ransom Project

Conclusion

Some of what you will do here will be extra steps for you and your team in your everyday work. Unfortunately, that is part of the price of improved security in light of the massive cyber threat we face in the 21st century. But excellent security can be far more seamless and productively rewarding if properly implemented and coupled with good training.

At NPC, we provide Secure Managed Computers™ that are secured, managed, and monitored for you, all for a single monthly fee. Combined with Microsoft 365, we can create an "Office of the Future™" for you that will take the worries away, giving you secure, productive computing.

Book a free consultation today with one of our NPC professionals, who will be pleased to answer any questions you may have and can advise how our solutions will benefit your business.

If you do decide to enjoy the benefits and security of our solutions, mention this whitepaper and get a free NPC Data Migration for your new system, a $195 CAD value, with our compliments.

Find out how NPC can help protect your small business from ransomware

Book a free secure computing consultation.

Book now

[1] Graham Cluely, "After hackers blackmailed their clients, Finnish therapy firm...", Bitdefender, 2021
[2] "The State of Ransomware 2024", Sophos, April 2024
[3] Melaine Maynes, "One simple action you can take to prevent 99.9 percent of attacks on your accounts", Microsoft, August 2019

Disclaimer: This document and any of the links attached is provided as a public service and should not be mistaken for legal or regulatory advice. The author and contributors assume no liability for its use. Free NPC Data Migration offer cannot be combined with any other offers or discounts. Taxes Extra. O.A.C. NPC reserves the right to cancel or amend this program offer at its discretion.

Copyright © 2025 NPC, NPC DataGuard, NPC DataGuard Pro and NPC logos are trademarks and/or registered trademarks of NPC DataGuard, a division of Compugen Inc. All rights reserved. All other trademarks cited herein are the property of their respective owners.