2022

Tips to Defend Against Ransomware

Learn what it takes to beat cyber criminals and save your business.

Introduction

Ransomware has ravaged businesses. A small slip up can lead to ransomware infecting your entire network and encrypting your data.

In 2021, ransomware brought down oil pipelines, government organizations, and a multi-billion dollar insurance company. Syndicates like Re-Evil, DarkSide, and Conti will target SMBs as well as big enterprises.

Its more important than ever your business remains vigilant. The average ransom payment in 2021 was $200,000 according to the NSI. Cyber Insurance premiums are skyrocketing and some like French insurance giant AXA have stopped paying ransom all together.

The situation is dire. But ransomware is not inevitable. Businesses that are prepared, enforce security protocols, and have tools in case an attack does occur can stand confidently in response to ransomware.

This E-book will provide several actionable tips your business MUST follow going into 2022.

TIP 1: USE 2FA

2FA (two factor authentication) adds an extra layer of protection to your organization. Once a password is entered correctly, 2FA requires an extra one-time password usually sent via email, text, or 2fa app. This means if a password is compromised a hacker will have a harder time breaching your infrastructure.

Most online accounts now provide the option to enable 2FA. Here are a few 2FA apps we recommend:

- **Authy** by Twilio
- **Google Authenticator**
- **Microsoft Authenticator** (for organizations using Office365)

TIP 2: Use SSO

Single Sign On (SSO) provides convenience and peace of mind to organizations. SSO allows administrators to control login access on all employee devices connected to the organizaton. This means if an employee becomes compromised or leaves, their password isn't at risk.

Popular SSO applications include:

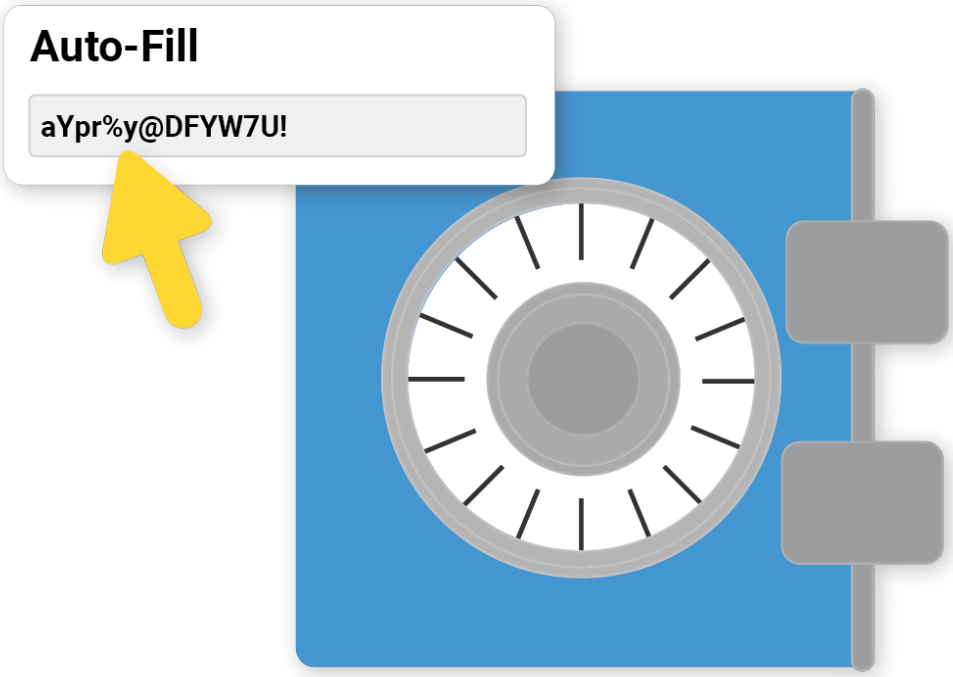
- **Okta**
- **Samba**
- **Microsoft Active Directory**
- **Kerberos**

TIP 3: Use Strong Passwords

Strong passwords are generally considered 12-20 characters in length and include at least 1 symbol, 1 capital letter, and 1 number. But the strongest passwords are composed of multiple of these in random sequence. Your password should never be something personal like your dogs name or old street address.

Here is an example of what we would recommend using for a password:
CqZb8qdq!bcSY#

See tip 4 for how to remember and generate strong passwords

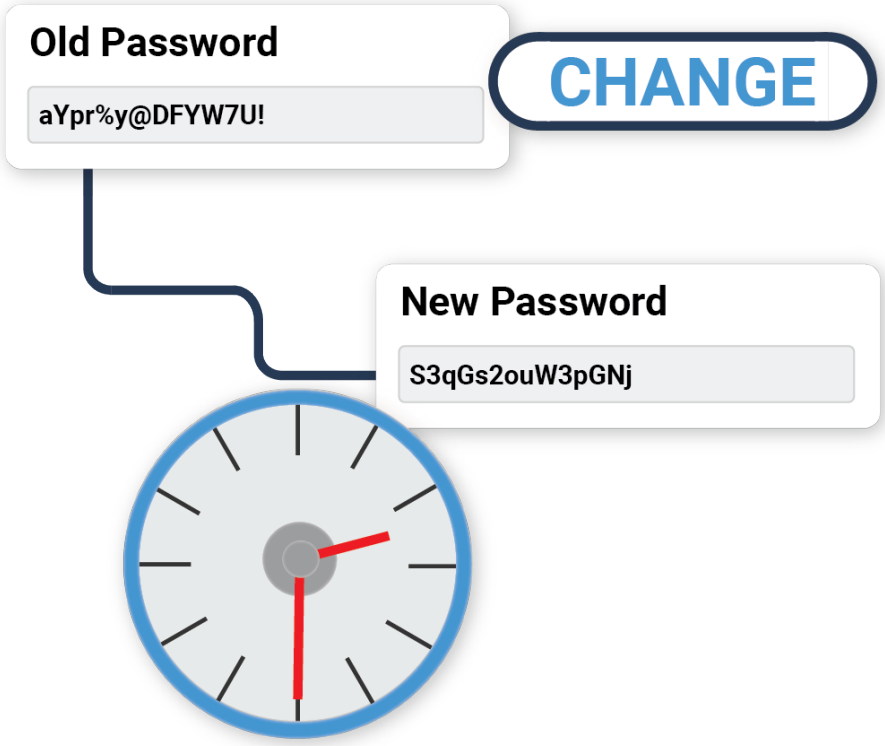


TIP 4: Use a Password Manager

Password Managers provide convenience and security. They save all user passwords in a secure place, allow users to auto-fill passwords into accounts as well as generate strong passwords in a click. Organizations can also manage who has access to what passwords and share them across the organization.

Many password managers are free for users and corporate accounts are inexpensive. Here are some recommendations:

- **Bitwarden** (Free and Open Source for users)
- **LastPass** (Free with limited functionality for users)
- **OnePassword** (Free trial available)

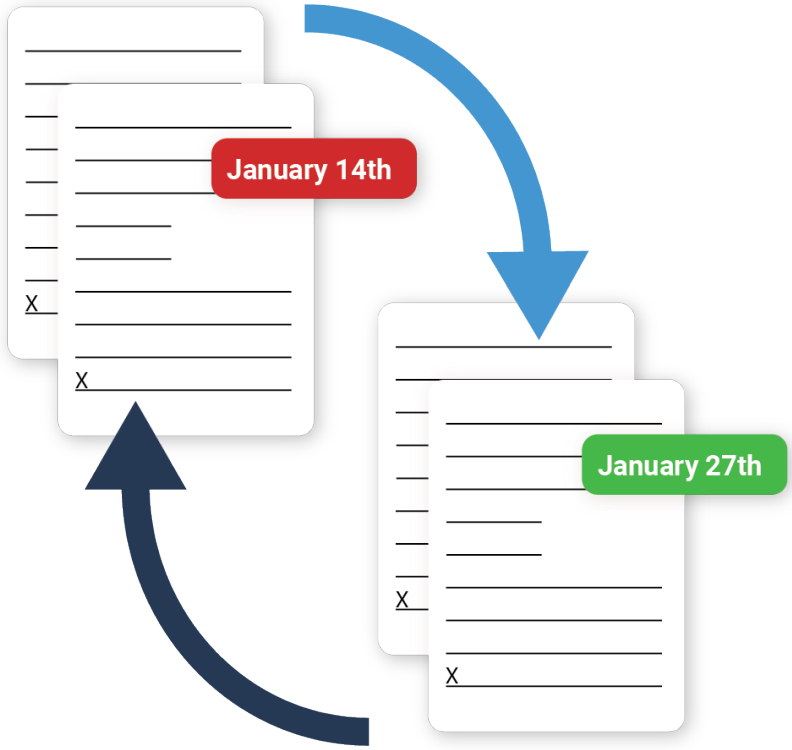


TIP 5: Require Password Changes

Cyber Criminals will have an easier time gaining access to your organization's critical data if your employees do not frequently change their passwords. We recommend that organizations require employees to frequently change their password. Employees should also not revert to old passwords after they are changed

Common intervals for changing passwords include:

- **Once per year**
- **Once per 6 months**
- **Once per quarter**



TIP 6: Use Backups

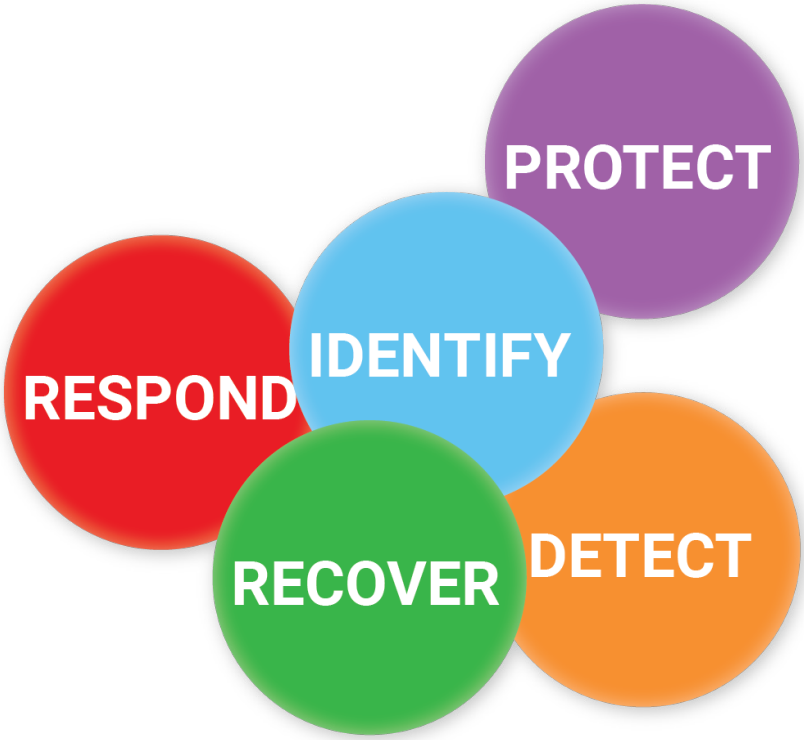
Backups do not prevent ransomware but might prove essential in recovering quickly from an attack. Backups (preferably immutable) allow your organization to revert to an older state before the ransomware encrypted your data. This allows your organization to avoid paying ransom.

If all your data is on desktops, you can backup your data to solid state drives and keep them offline in the office. Or use a desktop backup services like MSP 360. Those with servers or cloud solutions can rely on snapshots from the hypervisor or services like Carbonite.

TIP 7: Train Employees

Most ransomware still spreads through phishing emails. Meaning that downloading ransomware is mostly human error. Phishing emails and malicious websites are easy to spot. Proper training will ensure no employee downloads malicious code and infects your network.

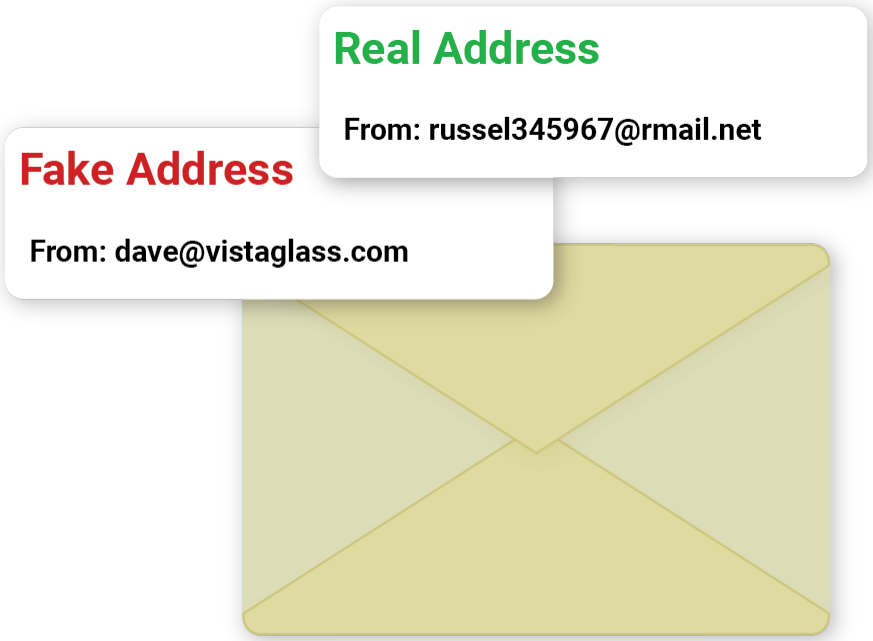
We recommend your organization invests heavily in training during the onboarding process for new hires and continues to train on new threats and existing best practices once a quarter.



TIP 8: Implement NIST

The NIST framework provides instructions on how to prepare, respond, and recover from a dire event like a ransomware attack. The framework is not specifically designed for ransomware attack preparation but instead allows your organization to assess your current security and assign responsibilities to keep your systems safe.

You can visit https://www.nist.gov/ for instructions on how to properly implement NIST.

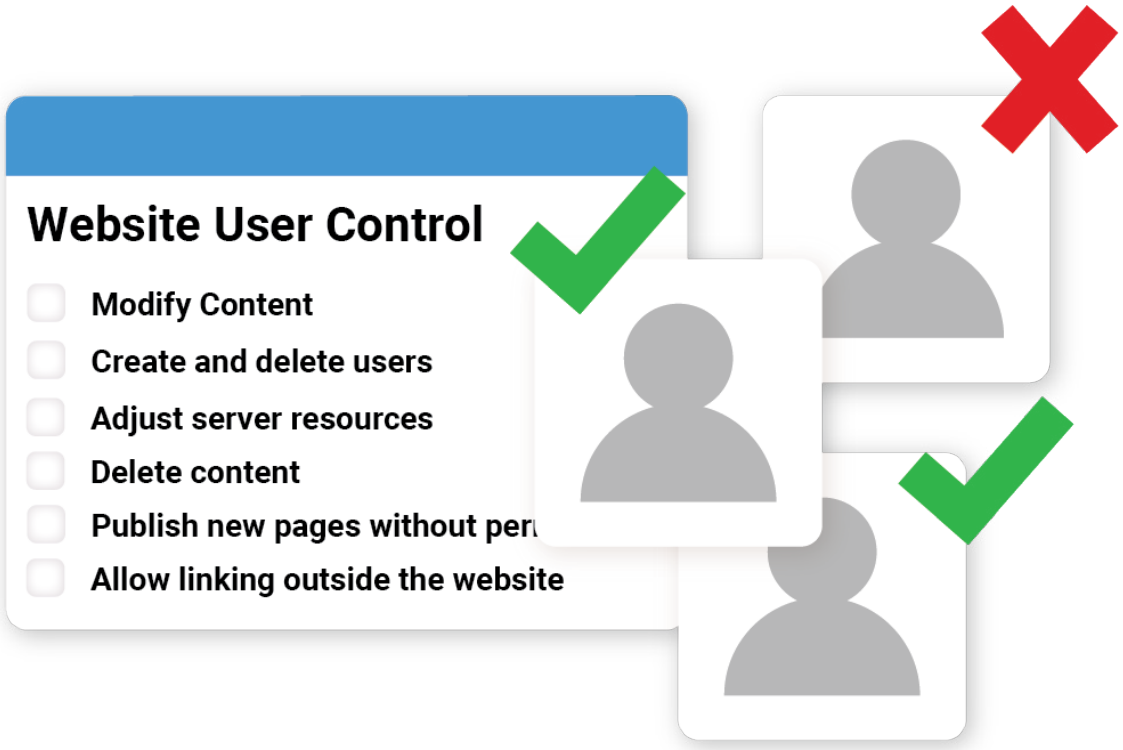


DKIM

TIP 9: Enable DKIM

A common way hackers infilitrate your employees' inbox is by posing as a higher up at your organization by spoofing their email domain. They can set their email to be something like jerry@ yourcompany.com. The hacker will then ask the employee to send credentials or download code.

DKIM provides extra authentication so your domain cannot be spoofed in an email. This means a hacker cannot set their email to show as youremployee@yourcompany.com. Zebra Cloud Mail supports DKIM if you are in need of secure email.



TIP 10: Review Access

Every business experiences turnover. You should periodically review which individuals have acces to critical business systems. For example, make sure a marketing manager that is no longer employed at your business does not have access to your WordPress site.

Failure to do so leaves a massive whole in your business' security. A disgruntled employee would have access to important systems and could login to plant ransomware directly on your systems, place malicious links on your website, or send malicious emails to staff.

TIP 11: Use a Ransomware Stopper

Zebra Ransomware Stopper prevents ransomware from encrypting your files. It does this by deploying decoy files that act like a trip wire. When ransomware begins an encryption process, ZRS files detects the encryption and stops it.

ZRS is also incredibly easy to install and manage across your organization. It installs like any other Windows program. Just download a simple .msi file and choose the folders you want defended. Then, manage all end-points from a single pane of glass.

Conclusion

Although ransomware has increased dramatically in the last few years, it doesn't affect businesses that are prepared and have a recovery plan if ransomware does strike.

The tips in this E-book provide your business with actionable items that do not require expensive consulting or IT solutions.

Most can be implemented for a low cost of even for free.

In fact, if your business works with a cloud provider like ZebraHost or an MSP, you can likely implement these solutions as a part of your normal services.

Services like 2FA, backups, and DKIM enabled email are to be expected from many cloud providers and MSPs.

If you are in need of secure services like ransomware protection, backup, or secure private clouds, ZebraHost offers several solutions and will customize a plan that works for your business.