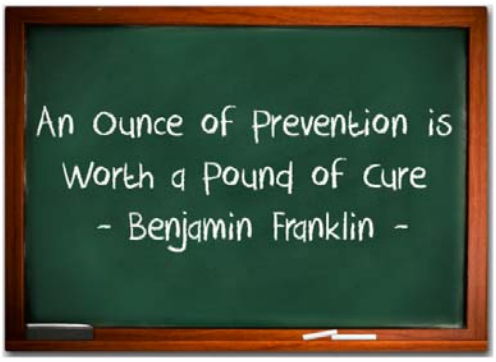

# The best data security and identity theft prevention methods for 2018

Be proactive and know what the crooks need to rip you off. Identify vulnerable points and take measures to protect yourself. An ounce of prevention is worth a pound of cure. You lock your door, why not your mail box? But why stop there? What about your email box and all the devices and vulnerable points in-between.

## Follow the Money

Identity theft and privacy concerns go hand and hand. For the crooks, it's all about getting the money, the easiest way possible and without getting caught. With today's technology it's easier than ever to get ripped off without you knowing until its way too late. It begins by having your personal information exposed. From there they can take out credit in your name, file an increased tax return and then steal your refund, access banking accounts and incur medical debt.




*"Prevent theft by protecting your sensitive information"*

The following list identifies sensitive personal information crooks need and how to secure it.

## Get a Locking Mailbox

Knowing that crooks need some sensitive personal information about you is the key to understanding how to prevent the theft in the first place.

Shred All Sensitive Documents and Junk Mail

Nothing identifiable goes in the garbage, EVER!

Freeze Your Credit

This will prevent someone else from getting credit with your identity because your credit report cannot be accessed, period!

Children's Credit

Equally important to remember is that your child's identity could also be stolen. It should be regularly monitored and there is no down side to freezing their credit.

Files Your Taxes Early

This will prevent others from filing a false return, usually an inflated tax return in an effort to steal the refund by beating them to the punch.

Don't Fall for Phone Scams

Don't reveal sensitive personal data especially your social security number, birth date, mother's maiden name, address, phone, email etc. Trust, but verify.

Online Shopping

Avoid using credit cards online whenever possible, instead use a PayPal account. This adds another layer of protection to avoid your credit card from being stolen online.

Disaster Recovery

Create a physical back up of your personal financial data such as credit card numbers. This will assist in the recovery efforts of lost or stolen data and will expedite your ability to notify your credit card company and prevent a loss.

Early Detection

Regularly monitor your credit, banking and medical records. This will only serve as an early warning system and will not prevent a loss.

Computers

Do not use administrative accounts for routine activities. These accounts are what hackers want to get because it will allow access to sensitive data and changes to settings and passwords.

Compartmentalize for Protection

Create separate user accounts and emails for online banking, shopping and surfing. This will prevent a breach from spreading to other compartments. Even consider using a separate device all together for your online banking because it's just too sensitive to risk.

Only Use Strong Passwords

Secure all computers with strong passwords that include a phrase, letters, numbers, uppercase and characters. Change regularly, and store manually in a password book, not in the computer.

Preventative Maintenance

Make sure your computer system has a firewall, antivirus and has the most recent security updates. Most of the cyber attacks target outdated security updates.

Separate Sensitive Data and Do Regular Back Ups

Keeping sensitive data off your computer used to browse or shop can prevent a potential loss if hacked and backing up your data regularly to an external drive will prevent data loss.

Two Step Authentications

This added level of security was developed for good reason and will prevent your sensitive data from being compromised.


Wi-Fi Use

Avoid public Wi-Fi because of their vulnerability. If you have your own Wi-Fi, disable the public broadcasting and change the factory default password to a strong one.

Data Encryption

Encrypting your data is a comprehensive method to prevent sensitive data leakage, just don't lose the decryption key!

Virtual Private Network (VPN)

A virtual private network extends a private network across a public network, and enables users to send and receive data across shared or public networks as if their computing devices were directly connected to the private network. A VPN is encrypted and more secure than a regular internet service provider.

HTTPS Everywhere

HTTPS is a Hypertext Transfer Protocol for secure communication over a computer network and HTTPS Everywhere is a browser extension that automatically redirects you to the HTTPS version of the website you are trying to visit.

Secure Mobile Devices

Establish a strong password; enable tracking and remote wiping capabilities. This will prevent your sensitive information from being accessed if lost or stolen.

Social Media

Enable all available privacy settings on all your social media accounts. Don't reveal any sensitive personal information, and check your sites regularly because updates made by the provider could default your profile to be open to the public until you re-set the privacy settings. Also don't participate in online survey test or games and avoid revealing any of your personal data to include two factor identification answers such as your mother's maiden name.


**For Business**

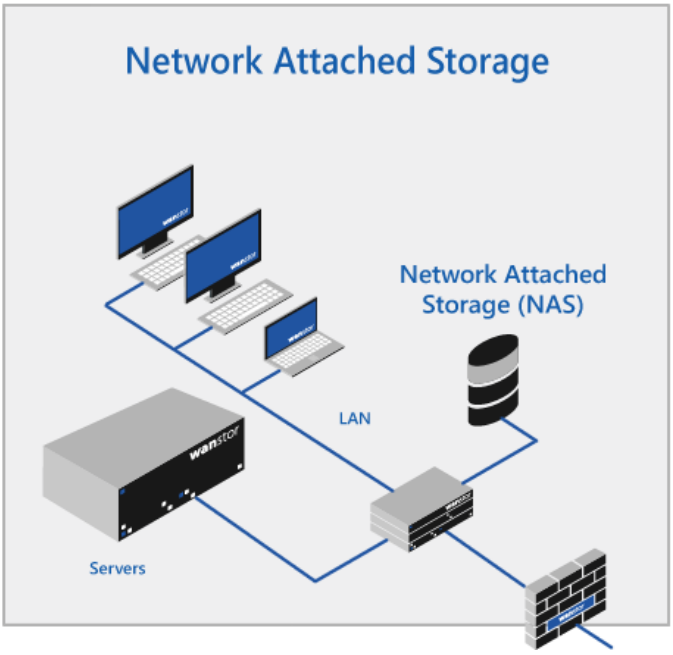
43% of cyber attacks happen to small businesses. In addition to all of the above recommended security measures to implement, here are some other tips for the small business owner.

Computer Use Policy and Security Awareness

Combined with the above security measures, having an effective internal policy and security awareness training will help keep employees out of sensitive areas and prevent possible cyber attacks from awareness about opening suspicious emails and attachments.

Network Attached Storage (NAS)

This is a cost effective way to handle not only data recovery plan by having data backups, but also goes to eliminate the possibility of getting stuck within a ransomware situation. It won't prevent a ransomware attack, but it will keep your back up system isolated and allow you to immediately recover without having to pay the ransom.




Web Sites

Again keeping up on all updates and security patches is the most important. Also enable the *Whois* privacy setting to mask your sensitive information. It's like having a non-published phone number.

Audit and Security Logs

This will monitor who is coming into your systems and what they may be leaving with. If there is a data loss from someone who had access to your network, such as a disgruntled ex-employee, these logs will capture the evidence needed to establish who took what, when, how and from where.

Isolate or Forensically Image All Devices of Ex-Employees

Combined with the audit and security logs, saving or isolating the hard drive from the devices used by the ex-employee will be a critical piece in establishing what data was lost or taken and when. Especially when the loss is discovered long after the employee left the company.

60% of Cyber Attacks on Businesses Occur Through 3rd Party Vendors

Make sure the companies you are doing business with are security savvy. Trust, but verify.

Prevention

Prevention is the key to avoid being a victim of a financial or intellectual property crime. It starts by knowing what the crooks need to rip you off and preventing them from getting access to it. If you need more information or help with a situation call now and speak with a certified digital forensic expert.


Contact an Expert

If you are not using a data backup system or don't have a network attached store NAS system to recover from a cyber attack your data is at risk. Call today to find out more about our data backup strategies and affordable custom NAS systems.