Interested in learning
more about security?

SANS Institute
InfoSec Reading Room

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

Protection of Customer Data For Home Business

I have family members starting a small home business and requesting advice on how to setup their home business computer. They will use their Windows XP laptop computer to record and process orders using the Internet. The request is to protect the customer data from physically or electronic miss use. Second, only authorized users will access customer data and restore any lost data. This report will respond to family members request or anyone else starting a small home business needing customer data protected.

Copyright SANS Institute
Author Retains Full Rights

AD

Protection of Customer Data

For Home Business

© SANS Institute 2003, Author retains full rights.

Written by David Davila
GSEC Practical Version 1.4b, Option 1
5 May 2003

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Table of Content

1. Introduction ---------- 4
1.1 Scope ---------- 4
2. Internet Access ---------- 4
2.1 Telephone Modem ---------- 4
2.2 DSL & Cable Modems ---------- 5
2.3 Recommendation ---------- 6
2.4 Security Issues ---------- 6
3. Personal Firewall ---------- 6
3.1 Overview ---------- 6
3.2 Recommendation ---------- 7
4. Antivirus Software ---------- 7
4.1 Overview ---------- 7
4.2 Configuration Procedures ---------- 7
4.3 Rules for Importing Files ---------- 8
4.4 Recommendation ---------- 9
5. Windows Security Updates ---------- 9
5.1 Overview ---------- 9
5.2 Procedures ---------- 9
6. Securing Windows XP ---------- 10
6.1 Overview ---------- 10
6.2 Logon Password ---------- 11
6.3 Disabling Accounts ---------- 11

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

6.4 Configure Screen Saver ---------- 12

6.5 Conclusion ---------- 13

7. Encryption ---------- 13

7.1 Overview ---------- 13

7.2 Pretty Good Privacy (PGP) ---------- 14

8. Data Recovery ---------- 14

8.1 Overview ---------- 15

9. Conclusion ---------- 16

10. References ---------- 17

© SANS Institute 2003, Author retains full rights.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

1. Introduction

I have family members starting a small home business and requesting advice on how to setup their home business computer. They will use their Windows XP laptop computer to record and process orders using the Internet. The request is to protect the customer data from physically or electronic miss use. Second, only authorized users will access customer data and restore any lost data. This report will respond to family members request or anyone else starting a small home business needing customer data protected.

1.1 Scope

This report will be limited to the Microsoft Windows systems. All examples used will be on Windows XP. You can assume the information provided will address other Windows systems unless otherwise noted. This report is broken into three parts. The first part *Internet Access* deals with options to access the Internet. The second part deals with protecting your system and personal data files from remote electronic access. The second part consists of the three sections *Personal Firewalls*, *Antivirus Software*, and *Windows Security Updates*. The third part deals with protecting your system and personal data files from physical hands-on access and recovery procedures for lost customer data files. The third part consists of the three sections *Securing Windows XP*, *Encryption*, and *Data Recovery*.

2. Internet Access

If your home business requires access to the Internet, you will have a choice of three access methods. For the home user, your choices will be telephone modem, DSL (Digital Subscriber Line), or cable modem. This section will address the advantages and disadvantages to each access method.

2.1 Telephone Modem

Most computers sold today come with an installed and configured telephone modem. To explain how a telephone modem works, the following definition is provided:

> Modem is an acronym for Modulator Demodulator. A modem is a device that converts data from digital computer signals to analog signals that can be sent over a phone line. This is called modulation. The analog signals are then converted back into digital data by the receiving modem. This is called demodulation.[1]

A home business on a limited budget could access the Internet using a telephone line and modem. Cost would be the major advantages, since most homes already have at least one telephone line installed. This would control expenses for the new home business during early operations.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

A second advantage is most computer purchases come with a modem pre-installed and configured for your system. Therefore, you do not have the added expense in purchasing a modem and get it installed. You also have the added benefit in shopping and comparing prices for the best Internet service provider in either your local area or one of the national companies.

The major disadvantage in accessing the Internet with a telephone modem is slow access speed. Most modem specification rates their speed at 56 kbps (kilobytes per second), but this rate is unachievable. The telephone system limits transmission speed to a maximum of 53 kbps with most common being from 33 kbps to 50 kbps. This means downloading large data files from the Internet will take longer compared to the other two methods described below. Therefore, the comparison is slow access speeds with a smaller startup cost compared to DSL and cable modem.

2.2 DSL & Cable Modems

The DSL and cable modem are referred as broadband connection with speeds of 256 kbps or faster. DSL uses existing telephone lines while cable modem uses existing television cable. The following definition states how DSL operates.

> DSL uses signal frequencies above those used by voice or fax, so the DSL signal does not interfere with telephone conversations or faxes. When a DSL filter is connected to your phone jack, its function is to split the data (Internet) traffic from voice (phone) traffic, and route them separately.
> Voice traffic (talking on the phone and fax signals) goes to the phone or the fax machine, while your data traffic (surfing the Web, downloading large files or photos) goes through the DSL modem and then to your computer, thus allowing you to use both at the same time.[2]

Like DSL, a cable modem provides high-speed access to the Internet. Cable modem sends its television signal to your set while data transmission goes to your computer. Data transmission does not interfere with television signals since both use different frequencies.

The major advantage to broadband connection is data speeds will be faster in comparison to a telephone modem. If you have requirements to conduct for example net meetings over the Internet, a high-speed connection would provide major improvement of performance and quality compared to a telephone modem. A second advantage would be faster downloading of large data files.

The major disadvantage to broadband connection is cost in both initial setup and monthly access fees. In the initial setup, you could need additional hardware. First, users might need an Ethernet network interface card installed and configured for your system. Second, additional DSL or cable modem hardware could be required. Third, you might have an additional fee for a service technician to visit your home to install and

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

configure your system. In addition, monthly access fees would be higher for either service compared to the first telephone modem option.

2.3 Recommendation

If high-speed access is your requirement, you will need to compare prices, additional hardware requirements, and shop for the best plan to meet your needs. My recommendation would be to start with a small investment. Therefore, a telephone modem connection would address most new home business requirements. You can review this decision as the home business grows and Internet access speed becomes an issue.

2.4 Security Issues

With Internet access, you are now part of the “World Wide Web” having just open up your customer data to the Internet and all of its “hackers”. To provide you with knowledge and skills in protecting your computer and customer data, this report will discuss personal firewalls, Windows XP security configuration, Windows security updates, antivirus software, encryption software, and data backup.

3. Personal Firewall

To protect your customer data and other computer information, you will need a layer of defenses. The external boundary to this defense is your personal firewall. This personal firewall is the first line of defense to prevent unauthorized Internet access from the net to your computer. Most firewalls also have the ability to prevent computer applications from accessing the Internet without your knowledge and approval.

3.1 Overview

Before computer data can travel on the Internet, the data needs to be placed in a fix packet size. This packet has a destination address, home address, and other information to reassemble the packets. A computer connected to the Internet will receive those packets from numerous sources without your intervention or knowledge, since your system is listening to numerous “ports”. A port allows a connection for computer applications to access the Internet. Therefore, one open port could allow a hacker to enter into your system and mount an attack on your customer data and other information.

Personal firewalls analyze all incoming packets and will only allow known and trusted packets to enter to your computer. This is done by allowing authorize port to remain open while closing any unwanted ports. If a hacker tries to access a close port, most personal firewalls would not acknowledge the port is closed. This makes your computer invisible resulting in the hacker having a hard time accessing your system and moving to another easier target.

Most personal firewalls monitor packets leaving your computer. This is important, since a malicious software code could try to send data to an unknown location without your

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

knowledge. A personal firewall will provide advance warning of this malicious application and prevent this data passing through the personal firewall. As a result, a personal firewall will control what applications are allowed to access to the Internet.

3.2 Recommendation

The industry has a wide selection of personal firewalls, but the two most common and favorites are BlackICE Defender (http://www.networkice.com) and ZoneAlarm (http://www.zonelabs.com). While both are great products, my recommendation and experience for a number of years is with ZoneAlarm. For a novice user, ZoneAlarm is easy to install and setup. The installation has a helpful computer base training on how the application works. ZoneAlarm is free for non-commercial use.

4. Antivirus Software

Your second layer of defense is the prevention of computer viruses. Computer viruses are a small software code written with the result to corrupt, delete, or make available your personal data files to the world. People write computer viruses in the hope to exploit flaws in the Windows operating system, applications, or computer hardware.

4.1 Overview

Computer viruses can be either annoying or cause major damage to your customer data files or Windows operating system. Here are a few actions computer viruses have performed in the past:

- It can keep your PC from booting up properly or loading Windows.
- It can make it impossible to run or open any files on your system.
- It can prevent your PC from recognizing certain types of hardware, including your hard drive.
- It can make Swiss chesses of your BIOS configuration, and it can surreptitiously send out infection-spreading e-mail to people in your address book.
- It can even disable your virus protection software, and in fact, many viruses are smart enough to do just that.[3]

4.2 Configuration Procedures

Protecting your system from a virus is a two-step process with the first step in installing and configuring antivirus software. Most new systems come with an antivirus application installed. If you do not have an antivirus application installed, the Recommendation sub-section will discuss the two favorite applications.

Antivirus applications require more than just installation and configuration. New viruses are written each day to exploit new computer flaws. An antivirus application has a built in database of known virus signatures. They use this database to compare known virus

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

signatures to your system's data files. Since new viruses are written each day to exploit new flaws, the virus signature database needs to be updated routinely.

Most antivirus applications check files being access by your system with its virus signature database. If a virus is detected, most will try to repair the file or at least quarantine the infected file or files. This would have limited affect if you do not have the latest virus signature updates. I have seen to many novice computer users who have installed and configured their antivirus application, but they have not updated the virus signatures since the first install. The leading vendor applications have setup an automated process to check and install new virus signature files into its database automatically.

There is a time gap between when a new virus is spreading and vendors have updated their virus signature database. This time gap could be a matter of a few hours to months later. Therefore, most antivirus applications have an automatic scan feature and will repair or at least quarantine the infected file or files. Antivirus software can go a long way helping in eliminating viruses form your system.

4.3 Rules for Importing Files

The second step is to reduce your exposure in being infected in the first place. By following a few basic rules about importing files to your computer, you can improve your chances in *not* getting your computer infected.

First, keep your virus signature database updated. With most applications performing this automatically, there is very little reason for most computers not to have the latest virus signature updates.

Second, have your application perform a virus scan daily. Again, most applications have a feature to perform this task automatically. Schedule this task when you know your computer will not be used.

Third, do not open an email attachment from anyone you do not know. This will prevent executing a virus on your system. The "I Love You" virus was sent by email and infected numerous systems around the world.

Fourth, all email attachments from known or unknown sources must be scanned before the attachment is opened. Most email applications have a feature to download a file attachment to a temporary folder. Once in this location, most antivirus applications can scan the selected file or files. Then again, some antivirus applications will work with the leading email software like Outlook or Outlook Express and will automatically scan your email attachments for viruses. Please review the type of applications being used. If you are not sure, download the attachment and scan the file or files will always work.

Fifth, when downloading files from trusted web sites, you should scan them before opening.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Sixth, you should not have any unknown floppy or CD disk from friends or software vendors loaded on your system without scanning for viruses. Yes, this includes software vendors. Remember the time gap between a virus being spread and vendors updating its virus signature database.

4.4 Recommendation

Most new computer systems sold are configured with an antivirus application. Normally, this application license has a limited period to update the virus signature database. After this period ends, you can extend this period by paying for automatic updates. If your computer system did not come with an antivirus application or the application does not have the needed features, you will need to purchase an application. Microsoft has a list of commercial software vendors in Microsoft Knowledge Base Article Q49500 at http://support.microsoft.com/default.aspx?scid=kb;en-us;49500.

On the other hand, the industry does have its favorites being "Norton AntiVirus" from Symantec (www.symantec.com) and VirusScan from McAfee (www.mcafee.com). While either of the two vendors would protect your customer data from viruses, I have used Norton AntiVirus for a number of years. Therefore, you should shop discount stores, the Internet, and the vendors' web sites for the best price. Some vendors' web sites will offer a free download for a limited period for your inspection.

5. Windows Security Updates

Put yourself inside a hacker's mind. If you want to have the biggest effect, would you try to attack computer systems that few users have or use? No, you would plan your attacks against the most popular operating systems being used with the largest install base. Therefore, Microsoft Windows operating systems enjoy the status as the hackers' primary choice. Microsoft combats hackers by fixing security flaws found by them and providing those fixes online to its customers free of charge. Therefore, your third layer of defense is to install the latest security fixes.

5.1 Overview

After an experienced hacker finds a security flaw with Windows, most would write a script to exploit this vulnerability. These new scripts find their way to hacker web sites to be used by less experience hackers to launch their own attacks. Those less experience hackers are referred in the industry as "script kiddies".

Once Microsoft is either informed of the security flaw or reviews the latest hacker scripts, they patch the security flaw and make the patch available in their website. Windows has a scan feature to provide a customize update specific to your system. This feature also updates other Microsoft application and device driver updates.

5.2 Procedures

How can you keep your system updated with the latest security updates? First, access the web site located in http://windowsupdate.microsoft.com. For Windows XP and other

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

version of Windows, you can also access the web site from Internet Explorer menu "Window > Updates".

Second, when displaying this web page, you will see a light blue "*scan for updates"* link. Click on the link and the web site will scan your system and provide a listing of customize updates specific to your system. The updates will be in three categories of "Critical Updates", "Recommend Updates", and "Device Drivers". Any available "Critical Updates" would automatically be selected for installation. For the other two categories, you will need to review and make your own selection.

Third after your selection, you will need to click the "Review and install updates" link. This section will display the listing of updates you selected and any critical updates. At this time, you can remove any listed updates. The last step would be to click the "Install Now" link.

Close all applications with the exception of Internet Explorer to update your system. Some updates may require a re-boot of your system before the updates take affect. If you were thinking this would put the script kiddies out of business, you would be wrong. Most security breaches come from known security flaws with fixes already provided by Microsoft.

6. Securing Windows XP

In the last three sections, we discussed how to protect customer data from remote electronic attacks. Those attacks can come for your next door neighbor or someone from the other side of the world. The third part of this report deals with protecting your system and personal data files from physical hands-on access and recovery procedures for any lost data files. This section *Securing Windows XP* and the sections of *Encryption*, and *Data Recovery* will complete the third part of this report.

6.1 Overview

Windows 95, Windows 98, and Windows Special Edition known as Win9X are mainly for home user with Microsoft replacing those systems with Windows XP. Therefore to ease the transition, the default settings for a newly install Windows XP system provides for little physical security. While the settings would be great for a system being used to play games or surf the web for fun, your system contains private customer data needs more protection than the standard default settings. Therefore, your fourth layer of defense is to secure Windows XP by preventing unauthorized persons with physical access to logon and access customer data

If you are still on a Win9X system, this section does not apply. For Windows NT and Windows 2000 systems, you will find useful information, but the examples will reference Windows XP systems.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

6.2 Logon Password

With Windows XP default settings, a welcome screen appears displaying one or more accounts created on this system. You click on the account and Windows XP continues the logon process. Therefore, anyone who has physical access to your system can access your customer private data. At this point, they can either delete the data or copy the data to include credit card numbers. To prevent anyone from turning on your system and accessing your data, a valid login ID and password needs to be entered before allowing the system to come online. To force a password during logon, the following is provided:

- Click on Start > Control Panel > User Accounts
- Click Change an Account
- Click the account you want to change
- Click Create Password
- Type the password you want to use, retype password to verify, leave the password hint blank *
- Click Create Password

*The object is to prevent anyone from logging into your system and accessing your customer data. Let us not provide them with a mean to crack your password by providing them with a hint. What makes a good password that is hard to crack?

First, a Windows password is case sensitive, meaning Windows will reject a password if the wrong case is used. Here are a few rules to remember when creating your password:

- The password should be at least seven characters long.
- The password should not contain a dictionary word.
- The password should include upper case, lower case, number, and special characters. Special characters are created by holding down the shift key and typing any of the number keys at the top of your keyboard.

6.3 Disabling Accounts

To protect customer data, unwanted computer accounts needs to disabled. For example, Windows XP creates an account named “Guest”. This account allows anyone to logon to your computer with limited access. Even with this configuration, you should restrict access to your system by anyone. To disable this account, the following procedures are provided:

- Click on Start > Control Panel > User Accounts
- If under Guest account the following statement appears “Guest Account is On”,
    - Click Guest account
    - Click “Turn off the Guest Account”
- If under Guest account the following statement appears “Guest Account is Off”
    - The account is disabled

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

With the window “Start > Control Panel > User Accounts” opened, you can review any other accounts. To delete an unwanted account, the following procedure is provided:

Click on Start > Control Panel > User Accounts

- Click “Change an Account”
- Click to select the account you want to change
- Click “Delete the Account”

If there is a chance the account might be needed at a later date, you might want to disabled the account and not delete it. The following procedure is provided:

- Click on Start > Control Panel > Administrative Tools > Computer Management
- Click on “Local Users and Groups” in left panel
- Double click on Users in right panel
- Click to select account you want to disable
- Click on Action menu then Properties
- Click to select “Account is disabled”

6.4 Configure Screen Saver

Screen saver was first used in the early years of computers to prevent a constant images being burnt onto a computer’s monitor. With Windows NT, Windows 2000, and now Windows XP; a security feature has been added. When the screen save comes on, your system is lockout until you type your logon password. By setting the number of minutes of inactivity, the screen saver will come on and prevent anyone from accessing your system and the customer data. By hitting the three keys CTRL+ALT+DEL together, a menu will appear to lockout your computer. Therefore, you can walk away with the computer turned on and no one can access your customer data without typing your logon password.

As with other security settings, the standard Windows XP default setting does *not* support the CTRL+ALT+DEL configuration. By setting the CTRL+ALT+DEL configuration, the default mode for Windows XP logon will also change. A logon screen will appear telling you to press the keys CTRL+ALT+DEL. A second screen appears for your user name (computer account) and password. Microsoft provides the following procedure for XP:

> To Enable or Disable the CTRL+ALT+DELETE Sequence
> 1. Click Start, click Control Panel, and then click User Accounts.
> 2. Click the Advanced tab.
> 3. In the Secure logon section, select or clear the require users to press Ctrl+Alt+Delete check box.[4]

If your Windows XP is configured like my system, the above procedure may not work, since your system may not contain an advanced tab as stated in step two. For those individuals, the following procedure will work.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

- Click on Start > Control Panel > User Accounts
- Click “Change the way users log on or off”
- Click to deselect “Use the Welcome screen”
    - The above step will also deselect “Use Fast user Switching”
- Click “Apply Options”

After clicking on “Apply Options”, you can press the keys CTRL+ALT+DEL. A Window will open and one of the options would be to lock your system. When your system is locked, you will need to press keys CTRL+ALT+DEL and type your password to access your system data. Even if you lock your system and for those who walk away without locking your system, I would highly recommend configuring the screen saver to require your password before accessing your system. The following procedure will configure your screen saver and require your logon password to access your system after the screen saver comes on:

- Click on Start > Control Panel > Display
- Click “Screen Saver” tab
- Select the type of screen saver you want by clicking on the down arrow
- Select 5 minutes or any other number for your wait time
- Click by selecting the box “On resume, password protect”

6.5 Conclusion

This section provides increased system security by preventing anyone with physical access to logon and access customer data. We discussed how to configure your system to force everyone to logon with a password. To prevent unknown persons from accessing your system, you were shown how to disable the guest account and delete or disable any other unwanted accounts. In the last step, your screen saver was configured so no one could access your data when the system was left on.

7. Encryption

If your system was stolen or lost, could someone recover your customer privacy data? If you follow the steps in the last section in setting a logon password and had a strong password, this could prevent someone with little knowledge of computer systems. In contrast, an experienced hacker could recover your data, even when a logon password was set. This area is known as computer forensics used by both law enforcement and computer hackers. All a person would need is the physical access to your system and the knowledge to use the correct forensic applications.

7.1 Overview

Your fifth layer of defense is to encrypt all customer data, so access to your system would prevent anyone from reading any data in clear text. Windows XP comes in two versions the Windows XP Home Edition and Windows XP Professional. The Home Edition is very similar to Professional with a few options removed. For example, the Windows XP Professional does have an Encrypting File System (EFS) to secure data.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Microsoft documentation states, "The EFS feature is not included in Microsoft Windows XP Home Edition".[5] For most home business, you would be using the Windows XP Home Edition, so this would not be an option. For those with Windows XP Professional, a review of Windows 2000 EFS provided the following information:

> We do not recommend using Win 2000's Encrypting File System for this role because it adds little additional authorization security to standard NTFS protections and is easily circumvented by dedicated attacker with physical access to the systems anyway (See Chapter 6).
> …One of our favorites is PGPdisk…[6]

7.2 Pretty Good Privacy (PGP)

PGP http://www.pgp.com is an encryption application first released by Phil Zimmerman in 1991 to send and receive encrypted email messages, since email messages sent by the Internet is like sending a post card to the US mail system. A number of people can read your message in either system. Mr. Zimmerman must have designed an outstanding encryption application, since the US Government filed charges in US court in 1993. The US court dropped the legal case against him in 1996.

From the early years, a freeware version of PGP to send and receive encrypted messages has been offered. The freeware license is for "not-for-profit activities".[7] Conversely, this license does provide the capability for your customers to send you an encrypted message containing privacy data like credit card information. The freeware version is only a subset of the commercial version. "PGP Personal for Windows 8.0.2" is the full version license for personal use and contains the PGP Disk.

> PGP Disk allows you to create disks whose contents are encrypted at all times. PGP Disk is particularly critical on laptops, which are increasingly vulnerable to being lost or stolen. By storing data using PGP Disk, users are assured that no unauthorized individual has access to it.[8]

When creating a PGP Disk, the encrypted data storage size is important for the Data Recovery section below. When creating the PGP Disk, you will be asked for the storage size of your disk. If the size is too small, not all your data can be stored. If the size is too big, you will have a harder time in the Data Recovery section. You can estimate the size of your current data in Windows XP by opening "Windows Explorer". Clicking on "Start> Run" and typing EXPLORER can perform this. After locating the folder where your customer data resides, move your mouse pointer to the folder and click the right button. A window will open and using the mouse pointer left click on "Properties". A window will open and the file size will display. Create your PGP Disk to cover the current storage and any future growth.

8. Data Recovery

You can lose your critical customer data from your computer other than being stolen or lost to include hardware failures, software failures, computer viruses, and computer

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

damage because of act of God or Mother Nature. USA Today states, “Fewer than 4% of computer users regularly back up their computers, says Jeff Zbar, an expert on home office security…”[9] Therefore, your sixth layer of defense is to plan on being in the 4% who can recover in lost data.

8.1 Overview

Data recovery can be broken into three steps. First, what data needs to be backed up? Second, what hardware and software will be used to backup the selected data? Third, where will the backup data be stored for later use?

If you followed the last section recommendations, all your important data is residing in an encrypted PGP Disk. Therefore, the data needing to be backup is in one encrypted file. A second folder needing to be backup is the PGP Keys. This folder is used to encrypted and decrypted messages and PGP Disk data. If PGP needs to be installed in a new system, you would need the PGP Keys to decrypt any messages from the old system. The PGP Keys folder is located under “My Documents” folder.

In the hardware used to backup your data, you will have a few options. In many computer systems sold today, a CD burner might be a standard option. The simplest method would be using the CD burner to create a folder and name the folder in the current number date format of YYYYMMDD. Backup the encrypted data and PGP Keys into the just created folder. This would allow you to easily identify when the backup took place for later restore. If you do not have a CD burner, you could use a zip drive. Again, create a folder using the current number date in YYYYMMDD.

Where will the backup disk reside? Best practice states should have the latest backup at your location, but the next oldest backup should be keep at an offsite location. If an act of God or Mother Nature destroys where the computer resides, your data and its backup would also be lost. If you keep the latest backup in your home, I recommend keeping the backup in a fireproof box. As for the next oldest backup, you can keep them with in a relative’s house or at work. Keeping your customer data offsite should not be an issue since it is encrypted.

Another method to backup customer data without using any hardware and offsite storage location is to use one of the online backup services. You would backup your encrypted data using your Internet connection. The three companies in this market are SwapDrive (www.swapdrive.com), Connected Corp (www.connnected.com), and NovaStor Corp (www.novastor.com). As always, you need to shop for the best deals. To help find the best deals, CNET provided the following rules:

> I still think that online backup is a good idea, provided you follow these rules.
>
> - Try before you buy. Make sure the service really works before you commit to more than a month, or look for services that offer free trials.
> - Check your files. Don't assume that your data is being backed up. Retrieve a few files at random to verify that they're being saved.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

- Clock your data restores. Some backup services store data on tape drives, which can make it impossibly slow to retrieve. You want to see how long it takes to restore data and make sure that the files come back intact.
- Ask about security. How does your backup service back up its servers? How does it protect your files from hackers and snoops? You want a site that backs up or mirrors your data to another location on at least a daily basis and one that encrypts the data using at least 128-bit encryption, for example. Find out before you entrust it with your data.
- Keep copies. Every month or so, copy your most important files to a Zip disk or a CD. You never know when your ISP will go down and leave you without access or whether your online backup provider will suffer a data disaster of its own.[10]

9. Conclusion

At the beginning of this report, we discussed the options to access the Internet and stated using the current installed telephone modem would be the best option for starting a new home business. The second part discussed how to secure your system from remote attacks from across the street or around the world by providing information on *Personal Firewalls*, *Antivirus Software*, and *Windows Security Updates*. In the third part, we discussed protecting your system and personal data from physical hands-on access and recovery procedures for any lost data files by providing information on of *Securing Windows XP*, *Encryption*, and *Data Recovery*.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

10. References

1. "Technical Reference InfoBase: Modem Overview." http://www.modem.com/glossary/glos24.html (5 May 2003)

2. "Learn How Verizon Online DSL High-Speed Internet Access Works." http://www22.verizon.com/ForHomeDSL/Channels/DSL/how+dsl+works.asp (5 May 2003)

3. Chase, Kate J. PC Disaster and Recovery. San Francisco: SYBEX, 2003. 81

4. Microsoft Knowledge Base Article – 308226. "HOW TO: Enable or Disable the CTRL+ALT+DELETE Sequence for Logging On in." 27 Oct 2002. http://support.microsoft.com/default.aspx?scid=kb;en-us;308226 (5 May 2003)

5. Microsoft Knowledge Base Article – 308989. "HOW TO: Encrypt a Folder in Windows XP."26 Oct 2002. http://support.microsoft.com/default.aspx?scid=kb;en-us;308989 (5 May 2003)

6. McClure, Stuart. Hacking Exposed: Network Security Secrets and Solutions, Third Edition. New York: Osborne/McGraw-Hill, 137

7. "PGP Freeware." http://www2.pgp.com/products/freeware.html (5 May 2003

8. "PGP Personal." http://www2.pgp.com/products/personal.html (5 May 2003)

9. Hopkins, Jims. "Tech Attacks are Big Challenge to Small Firms." Small Business. 9 Jan 2002. http://www.usatoday.com/money/smallbusiness/entre/entre.htm (5 May 2003)

10. Tynan, Daniel. "Online Backup: Be Careful Out There." Inside @ccess CNET's ISP Expert Weighs In. 28 Oct 2002. http://www.cnet.com/internet/0-3762-8-20593868-1.html (5 May 2003)

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Last Updated: May 25th, 2013

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

SANS Malaysia @ MCMC 2013	Cyberjaya, MY	Jun 03, 2013 - Jun 08, 2013	Live Event
SANS Pen Test Berlin 2013	Berlin, DE	Jun 03, 2013 - Jun 08, 2013	Live Event
Industial Control Systems Security Training - Houston	Houston, TXUS	Jun 10, 2013 - Jun 15, 2013	Live Event
Security Impact of IPv6 Summit 2013	Washington, DCUS	Jun 14, 2013 - Jun 16, 2013	Live Event
SANSFIRE 2013	Washington, DCUS	Jun 14, 2013 - Jun 22, 2013	Live Event
SANS Canberra 2013	Canberra, AU	Jul 01, 2013 - Jul 13, 2013	Live Event
Digital Forensics & Incident Response Summit 2013	Austin, TXUS	Jul 09, 2013 - Jul 16, 2013	Live Event
SANS London Summer 2013	London, GB	Jul 09, 2013 - Jul 16, 2013	Live Event
SANS Rocky Mountain 2013	Denver, COUS	Jul 14, 2013 - Jul 20, 2013	Live Event
SANS Mumbai 2013	Mumbai, IN	Jul 22, 2013 - Jul 27, 2013	Live Event
SEC528 SANS Training Program for the CompTIA® New Advanced Security Practitioner (CASP) Certification	Washington, DCUS	Jul 22, 2013 - Jul 26, 2013	Live Event
SANS San Francisco 2013	San Francisco, CAUS	Jul 29, 2013 - Aug 03, 2013	Live Event
SANS SEC 560: Network Penetration Testing @ Bangalore 2013	Bangalore, IN	Aug 05, 2013 - Aug 10, 2013	Live Event
SANS Boston 2013	Boston, MAUS	Aug 05, 2013 - Aug 10, 2013	Live Event
Critical Security Controls Summit	Washington, DCUS	Aug 12, 2013 - Aug 18, 2013	Live Event
Industrial Control Systems Security Training - DC	Washington, DCUS	Aug 12, 2013 - Aug 16, 2013	Live Event
SANS Thailand 2013	Bangkok, TH	Aug 19, 2013 - Aug 31, 2013	Live Event
SANS Virginia Beach 2013	Virginia Beach, VAUS	Aug 19, 2013 - Aug 30, 2013	Live Event
Mobile Device Security Summit 2013	OnlineCAUS	May 30, 2013 - Jun 06, 2013	Live Event
SANS OnDemand	Books & MP3s OnlyUS	Anytime	Self Paced