

# SECURITY BASICS

## Top 10 Security To-Do's

*Member and Employee Home Computer Security Guide*



Creating a more secure environment does not have to be difficult or costly. In fact, the level of security a member or employee enables can be greatly increased with a few simple product configurations and basic education.

The following pages outline ten areas to address to better increase

your security and greatly reduce your risk of falling prey to identity theft and becoming one of the 27 million victims.

Each one of the ten action items provides a brief description to help with understanding the issue and possible resources to help mitigate the threat.

### Security Facts

#### Is the ID Theft Threat Real?

A recently published study by the FTC stated that in the last five years over 27 million people in the United States have fallen prey to ID Theft. Of that, 27 million, 10 million became victims in the past one year.

#### Are Phishing Scams on the Rise?

According to MillersMiles, there were over 308 unique phishing email scams in the last 30 days (mid-Oct to mid-Nov).

#### What is the Big Deal with Phishing Scams?

Every 4 seconds an identity is stolen in the US.

\$8,000 is the average cost to restore a stolen identity.

600 hours is spent recovering from the crime.

### ID THEFT PROTECTION

ID Theft Protection enables members to engage in worry-free Internet transactions and browsing by simply registering your organization's domain through the free online manager. Members using the TraceAssure Toolbar will see your website as Authenticated and your credit union's name listed as well. This information allows your customers to browse without worry of fraud or identity theft. In addition, a free online security training portal is available to

educate end users on the risks associated with identity theft.

Protect your members and increase confidence in online banking by participating in the TraceAssure program. Upon certification your credit union will be able to add the TraceAssure Enabled logo to your web site.

For more information, visit:  
[www.tracesecurity.com](http://www.tracesecurity.com)



---

## ACTION 1: INSTALL ANTI-VIRUS

A virus is a manmade program or piece of code that causes an unexpected, usually negative event. Like biological viruses, computer viruses can spread quickly and are often difficult to eradicate.

In addition to replication, some computer viruses share another commonality; a damage routine that delivers the virus payload. While payloads may only display messages or images, they can also destroy files, reformat your hard drive, or cause other damage.

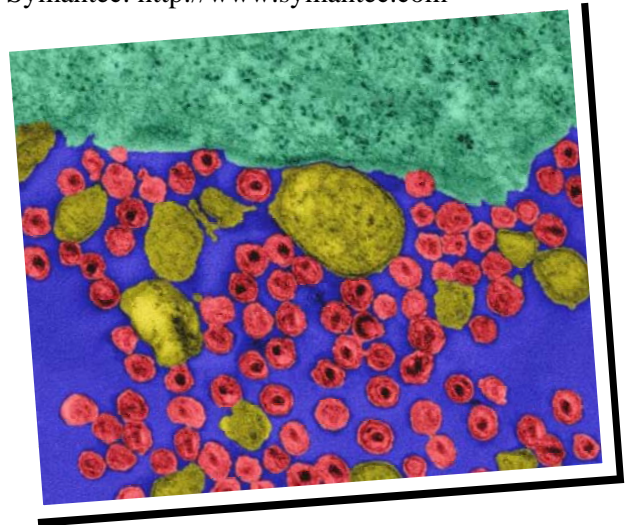
### Virus Detection and Prevention Tips

- Do not open any files attached to an email from an unknown, suspicious or untrustworthy source.
- Do not open any files attached to an email unless you know what it is, even if it appears to come from a dear friend or someone you know.
- Do not open any files attached to an email if the subject line is questionable or unexpected.
- Delete chain emails and junk email.
- Exercise caution when downloading files from the Internet. Ensure that the source is a legitimate and reputable one.

- Update your anti-virus software regularly.
- When in doubt, always err on the side of caution and do not open, download, or execute any files or email attachments.

### Resources:

- Grisoft: <http://free.grisoft.com> (AVG Free)
- Trend: <http://www.trend.com>
- McAfee: <http://www.mcafee.com>
- Symantec: <http://www.symantec.com>



---

## ACTION 2: INSTALL A FIREWALL

What is a firewall? A firewall is a logical or physical discontinuity in a network to prevent unauthorized access to data or resources.

In other words, it's like having a security guard at your front door to the Internet controlling internal and external access. Only those with the pre-defined right to enter or leave are allowed.

At minimum, enable the firewall built into Microsoft XP. If you choose to install a third party firewall that will provide more features and possibly be easier to manage, be sure to disable the Microsoft Firewall.

### Resources:

- ZoneAlarm: <http://www.zonelabs.com> (FREE)
- Kerio: <http://www.kerio.com>

---

## ACTION 3: SETUP MICROSOFT UPDATE



Microsoft Update is a Web site that offers downloads available from Windows Update plus the latest updates for Microsoft Office and other Microsoft programs.

When you visit Microsoft Update, it scans your computer and provides a list of updates. To sign up visit: <http://update.microsoft.com/microsoftupdate>.

---

## ACTION 4: SETUP EMAIL PROPERLY AND BE SMART

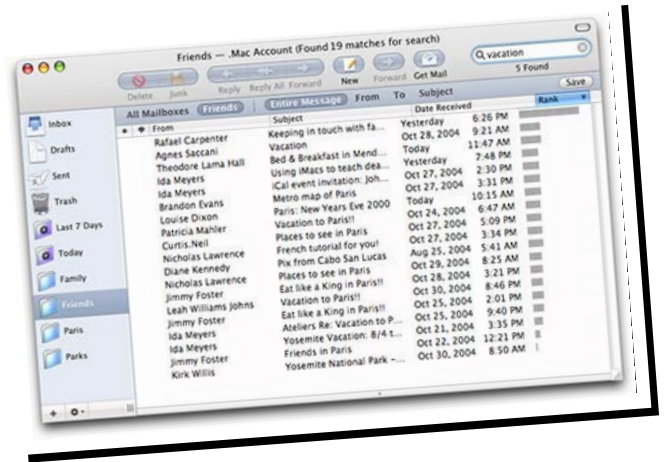
E-mail is a simple and effective vehicle for viruses and other malware attacks. In addition, unsolicited e-mails are used to capture email addresses for spam lists and possible identity theft attacks. To lower the risks follow these pointers:

- Do not open attachments unless absolutely necessary, especially if from an unknown sender.
- Do not open EXE, BAT, VBS, & SCR attachments.
- Always scan attachments with antivirus.
- Open up scanned attachments from within the program rather than double-clicking on it.
- If you are using Outlook/Express e-mail software configure e-mail messages as "Restricted Zone".
- Consider using a plain text e-mail reader.
- If possible, set your e-mail client to send messages in plain text.

- In Outlook/Express turn off AutoPreview.

### Resources:

- Setup Microsoft Security Tools
- WebRoot: <http://www.webroot.com>
- McAfee & Symantec



---

## ACTION 5: REGULARLY BACKUP YOUR FILES & FOLDERS



Setup your computer to backup your files regularly on ZIP disk, CD-ROM or Internet storage site. This will ensure that vital information on your computer will not be lost in the case of viruses, malware and general hardware failures.

### Resources:

- Software: McAfee & Symantec
- Hardware: CD/DVD Drive or External HardDrive. (<http://www.cnet.com>)
- Internet Solutions: iDisk, AT&T and more

---

## ACTION 6: STRONG PASSWORDS

Your living space has doors and windows, and perhaps most of the time they're locked. For each lock that uses a key, chances are that each key is different. You know to lock up and not to share the keys with strangers, and probably not with most of your friends. You also know that you should not hide the keys under the mat or in a flowerpot on your front porch.

Passwords for computers are much the same. For each computer and service you use (online purchasing, for example), you should have a password. Each password should be unique and unrelated to any of your other passwords. You shouldn't write them down nor should you share them with anyone, even your best friends.

### Resources:

Use a mix of characters, numbers and expressions. Search in Google for Online Password Generators.

---

## ACTION 7: USE CARE WHEN DOWNLOADING AND INSTALLING PROGRAMS

No matter how you acquire a program, it runs on your computer at the mercy of the program's author. Anything, any operation, any task that you can do this program can also do. If you're allowed to remove any file, the program can too. If you can send email, the program can too. If you can install or remove a program, the program can too. Anything you can do,

the intruder can do also, through the program you've just installed and run.

This is why when downloading music, programs and other executables from the Internet it is imperative that you scan the file with an updated antivirus solution before installing them. If you do not, the consequences can be dire.

---

## ACTION 8: SETUP WINDOWS ACCESS CONTROL



From Microsoft Web Site:

The access control feature in Windows XP Professional allows you to set a file or folder's access

permissions for a specific user, computer, or group of users. When you set permissions, you define the type and level of access granted to a user or group for a particular file or folder. For example, you can grant Read and Write permissions to the entire Finance group for the file payroll.dat. You can let one user read the contents of a file, let another user make changes to the file, and prevent all other users from accessing the file at all. To change permissions on a file or folder, you must be the owner of that file or folder, or you must have permission

to make such changes. You can also set similar permissions on printers so that selected users can configure the printer and other users can only print from it.

Resources:

- Microsoft:  
<http://www.microsoft.com/windowsxp/using/security/learnmore/accesscontrol.aspx>
- Crawler Parental Control (BETA):  
<http://www.crawlerparental.com>

---

## ACTION 9: FILE & FOLDER ENCRYPTION

If you store sensitive information on your computer, you should always consider using a file encryption program. Let's say for example, you store all your company's financial data on your personal or portable computer, losing it could allow someone else access to sensitive data that might hurt your business or you. If you are logged out of your account when your portable is lost, and file encryption is turned on, your business and personal information is safe.



Resources:

- PGP: <http://www.pgpi.org>
- Encryption Wiki: [http://www.infoanarchy.org/en/Hard\\_Disk\\_Encryption](http://www.infoanarchy.org/en/Hard_Disk_Encryption)
- Microsoft best practice for file encryption:  
<http://support.microsoft.com/kb/223316>
- NIST Cryptographic Toolkit:  
<http://csrc.nsl.nist.gov/CryptoToolkit/tkencryption.html>

---

## **ACTION 10: PROPERLY SETUP WIRELESS HOME NETWORKS**

Improperly setting up your home wireless network may have serious ramifications regarding your identity being stolen or your workplace being compromised. Taking the extra 15 minutes to sit down and enable the security measures that are standard with every wireless router is well worth the time.

It will reduce the likelihood of the potential security issues and add an additional layer of security to entice a potential hacker to move on to a less secure location.

### *Resources:*

- Wikipedia:  
[http://en.wikipedia.org/wiki/Wireless\\_security](http://en.wikipedia.org/wiki/Wireless_security)
- CNet: Wireless Made Easy...  
<http://www.cnet.com.au/wireless/0,239028844,240063340,00.htm>
- Microsoft:  
<http://www.microsoft.com/athome/moredone/wirelesssetup.mspx>

---

## **IDENTITY THEFT PROTECTION:**

**TraceSecurity TraceAssure** Eliminate the threat of Internet Fraud and Identity Theft

TraceAssure Toolbar not only supports two-factor authentication to online applications, but was also developed to eliminate:

- Phishing & Spear Phishing
- Pharming
- Man-in-the-Middle Attacks

TraceAssure was developed specifically for the home user with a focus on:

- Simple Setup
- Easy to Use
- **FREE**

How Does TraceAssure Work?

TraceAssure's groundbreaking patent-pending web authentication technology cross references every web page domain with the corresponding IP address. This information is validated against the secure TraceAssure "White List".

Participating sites that have been validated will display an "Authenticated" notification as well as post the name of the organization the user is visiting. If a malicious site attempts to impersonate a legitimate web site it will fail authentication and a "Malicious" message will be displayed. In addition, if a malicious site were to perform a man-in-the-middle type of attack, TraceAssure would catch the IP address difference and warn the user with a "Malicious" notice.

**To Download the Toolbar:** <https://www.tracesecurity.com/sa/download.cfm>

**To Enroll Your Credit Union:** <https://compliance.tracesecurity.com/TraceAssureSignUp.html>



---

## SECURITY TERMINOLOGY

### **Attack**

The act of exploiting a system's vulnerability.

### **Address spoofing**

A target system is "spoofed" into thinking that packets originated from places they did not.

### **Compromise key attack**

An attacker guesses cracks or obtains the key used for encryption/decryption and then captures that data.

### **Countermeasure**

Any mechanism that reduces vulnerability to a threat.

### **Data modification**

This occurs when traffic sent from point A to point B is intercepted in transit, modified and then forwarded to point B. Neither point knows that the traffic was changed.

### **Denial of service attack (DoS)**

The most common form of computer security breach is where an attacker floods a network interface with traffic to make the server so busy it cannot answer requests.

### **Degradation of service attack**

Known as "the new DoS", this hack decreases processing speed and might not initially be recognized as an attack. Because the effects are not immediately and dramatically evident, the attacks can go undetected for long periods.

### **Encrypt/Decrypt**

Encryption is the conversion of data into a form (called a cipher) that can not easily be intercepted by unauthorized users. Decryption converts data back to its original form.

### **End-to-end security**

A path that is encrypted from a client all the way to a destination server.

### **Firewall**

Computer hardware that prevents unauthorized access to private data (as on a company's local area network or intranet) by outside computer users on the Internet.

### **Hacker**

Any individual who attempts to attack, steal, distort, destroy, publish or otherwise compromise data on a computer system or network.

### **Internet Protocol (IP)**

Enables information to be routed from one network to another.

### **Internet Protocol Security (IPSec)**

A set of standards to deal with general attributes and policy regarding computer network security, encryption, authentication, keys and key exchange.

### **Internet Service Provider (ISP)**

A company that provides access to the Internet (as Time Warner Cable Business Class) for a monthly fee.

### **Logic bomb**

A computer virus set for a timed release. When the virus "detonates" it deliberately disrupts, modifies or erases data.

### **Malware**

A malware is a program that performs unexpected or unauthorized, but always malicious, actions. It is a general term used to refer to viruses, Trojans, and worms. Malware, depending on their type, may or may not include replicating and non-replicating malicious code.

Due to the many facets of malicious code or a malicious program, referring to it as malware helps to avoid confusion. For example, a virus that also has Trojan-like capabilities may be called malware.

### **Packet**

A unit of data that is sent across a network.

### **Router**

A device in a network that handles message transfer between computers.

### **Session hijacking**

This occurs when a session between source A and source B is intercepted and copied by an attacker.

### **Sniffer**

A device that captures all traffic going over the network.

### **Threat**

The potential exploitation of network vulnerability.

---

## **Trojan**

A Trojan is a malware that performs a malicious action, but has no replication abilities. Coined from Greek mythology's Trojan horse, a Trojan may arrive as a seemingly harmless file or application, but actually has some hidden malicious intent within its code.

Trojan malware usually have a payload. When a Trojan is executed, you may experience unwanted system problems in operation, and sometimes loss of valuable data.

## **Tunnel**

A link between tunnel client and tunnel server where data is encrypted and encapsulated.

## **Virtual Private Network (VPN)**

This is a network in which some parts are connected using the public Internet. However, the data sent across the Internet is encrypted so the entire network is "virtually" private.

## **Virus**

A computer virus is a program – a piece of executable code – that has the unique ability to replicate. Like biological viruses, computer viruses can spread quickly and are often difficult to eradicate. They can attach themselves to just about any type of executable file and are spread as files that are copied and sent from individual to individual.

In addition to replication, some computer viruses share another commonality: a damage routine that delivers the virus payload. While payloads may only display messages or images, they can also destroy files, reformat your hard drive, or cause other damage. If the virus does not contain a damage routine, it can cause trouble by consuming storage space and memory, and degrading the overall performance of your computer.

## **VPN Client**

Computer that initiates a VPN connection to a VPN server (also known as a tunnel client).

## **VPN Server**

Computer that accepts VPN connections from VPN clients (also known as a tunnel server).

## **Vulnerability**

Weakness in a system that can be exploited to violate the system's intended behavior. There may be vulnerabilities in security, integrity, availability and other aspects.

## **Worm**

A computer worm is a self-contained program (or set of programs) that is able to spread functional copies of itself or its segments to other computer systems. The propagation usually takes place via network connections or email attachments.

More recent worms have also discovered ways to propagate using Instant Messengers, via file sharing applications, and by collaborating with other malware such as Trojans or other worm variants.

WORM\_BAGLE.BE, for example, forms a vicious worm-Trojan cycle with TROJ\_BAGLE.BE, in which the worm mass-mails copies of the Trojan, and the Trojan downloads copies of the worm. Additionally, the FATSO family is a family of worms that propagate via an instant messaging application and a popular peer-to-peer file sharing application.

Some worms may have an additional payload, such as preventing a user from accessing antivirus Web sites, or stealing the licenses of installed games and applications.