

Online Security and Safety

Protect Your Computer - and Yourself!



STATE CREDIT UNION

www.scscu.com

Fraud comes in many shapes and sizes, but the outcome is simple: the loss of both money and time. That's why protecting your computer and your privacy is so important. Take action and get a peace of mind.

TABLE OF CONTENTS

PROTECT YOUR COMPUTER	PROTECT YOURSELF
3 Antivirus Software	11 Email Safety
5 Anti-Spyware Software	13 Online Identity Protection
7 Firewall Protection	15 Offline Identity Protection
9 Software Updates	17 Take Away Tips

Antivirus Software

Antivirus software detects and responds to various types of malware, including viruses, worms, and other programs designed to damage or disrupt a computer.



WHY

About Malware

Malware (malicious software). A general term used to describe any program designed to cause harm. Some common types of malware include viruses, worms, and trojans.

Virus. A malicious program that attaches itself to and “infects” other software applications and files, disrupting computer operations. Viruses often carry a “payload,” which is an executable script designed to damage, delete, or steal information from a computer.

A virus is a self-replicating program, meaning it copies itself. Typically a virus only infects a computer and begins replicating when the user executes a program or opens an infected file.

Viruses spread from computer to computer only when users unknowingly share infected files. For example, viruses can spread when users send emails with infected documents attached.

Worm. A worm is similar to a virus but with an additional dangerous element.

Like a virus, a worm can make copies of itself, but it does not require a person to send it along to other computers. A worm spreads rapidly across a network without having to attach itself to another program.

Since worms are so quick and pervasive through a network, they quickly absorb resources and can bring not just one computer down, but thousands, potentially shutting down an entire network.

Trojan. A malicious program disguised or hidden within another program that appears to be safe (much like the myth of the Trojan horse). When a trojan is executed, it allows attackers to gain unauthorized access to the computer in order to steal information and cause harm. Trojans commonly spread through email attachments and Internet downloads.

Fraud operators are constantly developing new viruses, spyware, and online fraud schemes; that’s not going to change. The good news is that most damage can be avoided with a combination of Antivirus and Anti-Spyware software, firewalls, and education.

2007 Identity Fraud Survey Report, Javelin Strategy & Research, February 2007

Antivirus software typically works in two ways...

Removes Known Malware

Antivirus software examines your computer looking for known viruses using a library of definitions and cures to remove threats. Antivirus software will automatically update its library to stay current as new threats and protections emerge.

Prevents New Malware

Antivirus software looks for suspicious computer processing behavior to prevent threats that are either new variants of existing threats or brand new threats altogether. Antivirus software prevents suspicious code from executing and blocks access to infected files.



HOW

How do I get Antivirus software protection?

Antivirus software can be purchased at an electronics store, online or offline.

Some Antivirus vendors include:

- Microsoft Security Essentials www.microsoft.com
- Symantec www.symantec.com
- McAfee www.mcafee.com
- Trend Micro www.trendmicro.com

How do I know if I already have Antivirus software?

Check the list of programs on your computer to verify if an Antivirus software is already installed. Look for program names that may match one of the Antivirus vendors above.

How long does Antivirus software last?

Most Antivirus vendors sell a perpetual license that requires annual renewal in order to continue receiving updates that protect against the latest threats. The annual renewal fee is often less than the initial purchase of the Antivirus software.

How do I update my Antivirus software?

Antivirus software automatically updates itself with the latest threat and cure definitions and often repairs damaged content automatically if it encounters malware (malicious software).



CHECKLIST

How to Protect Your Computer

- Install Antivirus software on your computer.
- Keep your Antivirus software license current.
- Only open email and attachments from known senders.

If you receive an attachment from someone you do not know or are not expecting, do not open it; delete it.

Anti-Spyware Software

Anti-Spyware software protects against another kind of malware, called spyware.



WHY

About Spyware

Spyware is a type of program that monitors a user's computer activity, collects information about a user without their knowledge, and then provides that information to a third party.

Spyware can be benign (like collecting information in order to show the user a targeted advertisement) or malicious (such as attempts to commit fraud).

The most dangerous spyware is usually combined with a trojan or

other malware and spread by criminals trying to obtain passwords, user IDs, account numbers, and other sensitive data in order to commit fraud.

Most spyware finds its way onto computers via the Internet. Web downloads and JavaScript files are popular ways to transmit spyware as they can be embedded in other programs and are self-executable, meaning they execute without any assistance from the user.

The highest average dollar losses in a 2007 survey of identity theft victims were attributed to malware (viruses, worms, trojans), spyware, computer hacking and phishing (email fraud).

2007 Identity Fraud Survey Report , Javelin Strategy & Research, February 2007

Anti-Spyware works much like Antivirus software

Prevents Spyware

Anti-Spyware software prevents spyware programs from collecting information on your computer and providing it to unknown parties.

Detects and Removes Spyware

Anti-Spyware software detects and removes spyware from your computer using a library of software file definitions and cures.



HOW

Where do I get Anti-Spyware software protection?

Anti-Spyware software can be purchased at an electronics store, either online or offline.

Some Anti-Spyware software vendors include:

- **Malwarebytes** www.malwarebytes.org
- **Microsoft** www.microsoft.com
- **Symantec** www.symantec.com
- **McAfee** www.mcafee.com

How do I know if I already have Anti-Spyware software?

Check the list of programs on your computer to verify if Anti-Spyware software is already installed on your computer. Look for program names that may match one of the vendors listed above.

Is spyware more dangerous than malware (viruses, worms, trojans)?

Spyware collects data and shares it with outside parties without your knowledge. It's made more dangerous when combined with malware and spread by cyber criminals. That's why it's important to have both Antivirus and Anti-Spyware protection.

Can I combine Antivirus and Anti-Spyware software?

Most Antivirus software vendors offer protection from spyware within their products or as a separate purchase. Be sure to verify that Anti-Spyware protection is included, or purchase a separate Anti-Spyware software package.



CHECKLIST

How to Protect Your Computer

- ✓ Install Anti-Spyware software on your computer.
- ✓ Keep your Anti-Spyware software license current.
- ✓ Read software agreements to understand exactly what applications are being installed on your computer.

Only download items from trusted sources.

Firewall Protection

Firewalls are systems that help prevent unauthorized access to and from computers.



WHY

About Firewalls

Firewalls help protect against attacks across any network - the Internet, your home network, and even wireless networks, like at the airport, library, or work.

There are two types of firewalls:

Software Firewalls are popular for individual home use. In fact, operating systems like Microsoft Windows and Mac OS often come

with built-in software firewalls. If not already “built-in” to a computer, software firewalls can be loaded onto any user’s computer.

Hardware Firewalls provide a strong degree of protection and are often used by businesses or users with networked computers. These physical devices require a power source and connect directly to a network.

Fraud operators are constantly developing new viruses, spyware, and online fraud schemes; that’s not going to change. The good news is that most damage can be avoided with a combination of Antivirus and Anti-Spyware software, firewalls, and education.

2007 Identity Fraud Survey Report , Javelin Strategy & Research, February 2007

How do I ensure my Firewall is working?

Where do I get a firewall?

Microsoft Windows, Mac OS, and even Antivirus software programs often include firewalls. Firewalls can also be purchased at most electronics stores. You can obtain free firewalls online although they offer minimal or non-existent technical support and documentation.

How do I know if I already have a firewall?

Operating systems often come with built-in software firewalls:

Microsoft Windows users can verify if the firewall is turned on by accessing the Control Panel > Windows Firewall.

Mac users can verify if the firewall is turned on by accessing System Preferences > Sharing > Firewall.

Do I need to maintain or update my firewall once it’s installed?

Check your system to ensure that the firewall is not only installed but also turned on.

What will happen if I don’t have a firewall?

Without a firewall, your system may be vulnerable to unauthorized access and attack.

Do I need a software firewall or a hardware firewall?

Most individual home users are suited to use a software firewall, typically the one that is included with their computer operating system. Hardware firewalls are typically suited for businesses and networked computers.



HOW



CHECKLIST

How to Protect Your Computer

Check your operating system to verify that your firewall is turned on.

If you don’t have a firewall, install one.

Use a firewall in conjunction with Antivirus and Anti-Spyware software.

Software Updates

Software Updates are necessary when companies identify application errors or weaknesses in their software or system that require stronger security protections.



WHY

About Software Updates

Software Updates come in the form of software “patches” that replace defective sections of software code with corrected code. All software manufacturers issue patches either on a regular schedule or as defects are discovered.

Malware such as viruses, worms, and trojans can infiltrate a computer through a software application that has not been patched.

Automatic Updates are included in most operating systems and

software programs. These features periodically and automatically update the user’s computer.

Microsoft Windows calls this feature “Auto Update.”

Mac OS calls this feature “Software Update.”

Other software programs may display pop-up notices within a program notifying you to install the latest software patches.

Software that’s not regularly updated can leave your computer system vulnerable to attacks.

How do I keep my computer up to date?

How do I keep my software programs updated?

Some programs, including Microsoft Windows and Mac OS operating systems, provide automatic software updates. Keep these automatic updates turned on so that your computer is protected routinely.

How do I check my computer operating system’s automatic update settings?

Microsoft Windows users can check the “Auto Update” settings by accessing the Control Panel > Automatic Updates.

Mac OS users can check the “Software Update” settings by accessing the System Preferences > Software Update.

How do I manually patch one of my software programs?

Most software programs have automatic update and patching features. The program’s “Help” menu may also include a feature allowing you to manually “Check for Updates.”



HOW



CHECKLIST

How to Protect Your Computer

- ☑ Check your automatic update settings to ensure you’re receiving updates.
- ☑ Check software updates that may be available in the “Help” menu or on the vendor’s website.

Pay attention to pop-up messages within a program; these may be notices of available updates.

Email Safety

Email safety means following best practices when you send and receive email.



WHY

About Email Safety

Email commonly transports malware, like viruses, that can result in identity fraud or computer damage. In addition to the transmission of malware, phishing also threatens email users.

Phishing is a type of email fraud in which the perpetrator poses as a legitimate, trustworthy business in order to acquire personal and sensitive information, like passwords or financial data.

Following some simple guidelines can help you safeguard your email environment.

It's never too late to evaluate your approach to email and develop good habits to protect your privacy, identity, data, and computer.

Practice safe email habits.

Never include sensitive information in email. Forged email purporting to be from your financial institution or favorite online store is a popular trick used by criminals to extract personal information from fraud.

Never open or respond to SPAM (unsolicited bulk email messages). Delete all SPAM without opening it. Responding to SPAM only confirms your email address to the spammer, which can actually intensify the problem.

Never click on links within an email. It is safer to retype the web address than to click on it from within the body of an email.

Don't open attachments from strangers. If you do not know the sender or are not expecting the attachment, delete it.

Don't open attachments with odd filename extensions. Most computer files use filename extensions such as ".doc" for Word documents or ".jpg" for images. If a file has a double extension like "heythere.doc.pif" it is

highly likely that this is a dangerous file and should not be opened. In addition, do not open email attachments that have file endings of ".exe," ".pif," or ".vbs." These are filename extensions for executable files and could cause damage to your computer if opened.

Never give our your email address to unknown websites. If you don't know the reputation of a website, don't assume trust. Many websites sell email addresses or may be careless with your personal information.

Don't believe the hype. Many fraudulent emails contain urgent messages claiming your account will be closed if sensitive information is not provided immediately or that important security information needs to be updated online.

Be aware of bad grammar, spelling, and design. Fraudulent emails and websites often include typos and grammar emails as well as unprofessional design layout and quality.



HOW



CHECKLIST

How to Protect Yourself

- Don't include sensitive information in email.
 - Never click on links within an email.
 - Don't open SPAM or attachments from strangers.
 - Be suspicious of emails asking for personal information.
- Be selective when providing your email address.

Online Identity Protection

Online Identity Protection means following best practices to help you browse the Internet safely and securely.

Online identity theft is on the rise, nearly doubling from 8.3% in 2006 to 16% in early 2007.



WHY

About Online Identity Protection

Online security includes following best practices while you're banking online, shopping, or just surfing the Internet.

Following simple guidelines can help protect your identity and allow you to conduct business online with confidence.

Practice safe habits to protect your identity online.

Be selective about where you surf.

Not all websites are benign. Sites that are engaged in illegal or questionable activities often host damaging software and make users susceptible to aggressive computer attacks.

Use a secure browser. Always use secure web pages when you're conducting transactions online. Look for "https://" at the beginning of the URL and/or a green padlock in the address area to verify the security of the site.

Select a strong password. The best password is an undetectable one. Never use birth dates, first names, pet names, addresses, phone numbers, or Social Security numbers as your password. Instead, use a combination of letters, numbers, and symbols. Be sure to change your passwords regularly.

Don't share passwords. Don't share your passwords with other people, of course, but also don't share passwords between sites. Set a unique password for each site.

Don't choose "Remember My Password."

You should never use the "remember password" feature for online banking or transactional websites.

Work on a computer you trust.

Firewalls, Antivirus, and Anti-Spyware software will help protect your computer and your personal information.

Don't use public computers for sensitive transactions.

Since you cannot validate the computer's integrity, there's a higher risk of fraud when you log in from a public computer.

Log off, disconnect, and shut down.

Always sign off from online banking or any other website that you've logged into with a user ID and password. Utilize automatic timeout features that prevent others from continuing your online banking session in case you leave your computer unattended without logging out. When a computer is not in use, disconnect it from the Internet or shut it down.



HOW



CHECKLIST

How to Protect Yourself

- Update and strengthen the security of your passwords.
- Use a secure browser and trusted computer for sensitive transactions.
- Log off when you're done using websites that require a user ID and password.

Disconnect and shut down when you're not using your computer.

Offline Identity Protection

Offline Identity Protection means following best practices to help you secure your personal information in the “real world.”



WHY

About Offline Identity Protection

Offline security is critical to helping you protect your identity. While online security is an important and current issue, the majority of identity fraud continues to take place offline.

Following simple guidelines for offline activities can help you protect your privacy and your identity.

The majority of identity theft and privacy infringement is the result of “real world” fraud, including lost or stolen wallets, checkbooks, credit cards, and stolen confidential information.

2007 Identity Fraud Survey Report , Javelin Strategy & Research, February 2007

Protect your identity in the “real world” too.

Lock your mailbox. Preferably, your personal mailbox should lock. Don’t leave mail in your mailbox longer than necessary - especially if your mailbox doesn’t have a lock.

Hold your mail. If you’re traveling, don’t let mail pile up. Have the post office hold your mail at times when you won’t be able to collect it.

Monitor mail closely. Take immediate action if bills do not arrive as expected or if you receive unexpected credit cards or a mysterious account statement.

Don’t give out your phone number. Ask solicitors or other businesses for their phone number so you have control over these communications.

Don’t give our personal information in surveys. Surveys, both online and offline, can be dangerous if they ask you to provide confidential information.

Safeguard your Social Security Number. Do not publish your Social Security Number on checks or other public documents. Do not carry your card with you; keep your Social

Security card in a safe place at home.

Copies aren’t necessary. Know your rights regarding copies of your driver’s license. Business transactions, like checking into a hotel, do not require a copy of your driver’s license.

Take advantage of free annual credit reports. Credit reports contain information about your accounts and your bill paying history. Major nationwide consumer reporting companies are legally required to provide free copies of your credit reports. Review your credit report each year for accuracy.

Shred, shred, shred. Shred bills, bank statements, pre-approved financial solicitations and other confidential information before discarding them.



HOW



CHECKLIST

How to Protect Yourself

- Monitor your postal mail.
- Don’t give our your personal information freely.
- Check your credit report annually.

Shred documents containing personal information before discarding them.

Protect Your Computer

✓ CHECKLIST

Antivirus Software

- ✓ Install Antivirus software on your computer.
- ✓ Keep your Antivirus software license current.
- ✓ Only open email and attachments from known senders.
- ✓ If you receive an attachment from someone you do not know or are not expecting, do not open it; delete it.

✓ CHECKLIST

Anti-Spyware Software

- ✓ Install Anti-Spyware software on your computer.
- ✓ Keep your Anti-Spyware software license current.
- ✓ Read software agreements to understand exactly what applications are being installed on your computer.
- ✓ Only download items from trusted sources.

✓ CHECKLIST

Email Safety

- ✓ Don't include sensitive information in email.
- ✓ Never click on links within an email.
- ✓ Don't open SPAM or attachments from strangers.
- ✓ Be suspicious of emails asking for personal information.
- ✓ Be selective when providing your email address.

✓ CHECKLIST

Online Identity Protection

- ✓ Update and strengthen the security of your passwords.
- ✓ Use a secure browser and trusted computer for sensitive transactions.
- ✓ Log off when you're done using websites that require a user ID and password.
- ✓ Disconnect and shut down when you're not using your computer.

✓ CHECKLIST

Firewall Protection

- ✓ Check your operating system to verify that your firewall is turned on.
- ✓ If you don't have a firewall, install one.
- ✓ Use a firewall in conjunction with Antivirus and Anti-Spyware software.

✓ CHECKLIST

Software Updates

- ✓ Check your automatic update settings to ensure you're receiving updates.
- ✓ Check software updates that may be available in the "Help" menu or on the vendor's website.
- ✓ Pay attention to pop-up messages within a program: these may be notices of available updates.

✓ CHECKLIST

Offline Identity Protection

- ✓ Monitor your postal mail.
- ✓ Don't give out your personal information freely.
- ✓ Check your credit report annually.
- ✓ Shred documents containing personal information before discarding them.

🏠 CONTACT

Contact State Credit Union

📍 PO Box 726, Columbia, SC 29202

☎ (803) 343-0300 (Local)

(800) 868-8740 (Toll-Free)

🌐 www.scscu.com

✉ info@scscu.com

📘 www.facebook.com/statecreditunion

🐦 www.twitter.com/scuconnect

