Antivirus Software

Antivirus software detects and responds to various types of malware (malicious software). Malware includes viruses, worms and other programs designed to damage or disrupt a computer system.

Where do I get Antivirus software protection?

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

*Some Antivirus software vendors include:

Symantec – www.symantec.com
McAfee – www.mcafee.com
Trend Micro – www.trendmicro.com
Avast! – www.avast.com
AVG – www.free.avg.com

How do I know if I already have Antivirus software?

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

*Vendors not affiliated with Navigant Credit Union.

Anti-Spyware Software

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

Where do I get Anti-Spyware software protection?

Anti-Spyware software is available at any electronics store, either online or offline.

*Some Anti-Spyware vendors include:

Symantec – www.symantec.com
McAfee – www.mcafee.com
Microsoft – www.microsoft.com
Webroot – www.webroot.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.

Software Updates

Software Updates come in the form of software "patches" that replace defective sections of software code with corrected code.

How do I keep my software programs updated?

Some software programs, including Microsoft Windows and Mac 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 or Windows Updates.
- Mac users can check the "Software Update" settings by accessing 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 "Help" menu may also include a feature allowing you to manually "Check for Updates."

Firewall Protection

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

Where do I get a firewall?

Microsoft Windows and Mac operating systems and even Antivirus software programs often include firewalls. Firewalls can also be purchased at most electronics stores or online. You can obtain free firewalls online; however, 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?

Your system may be vulnerable to unauthorized access and attack.

Do I need a software firewall or a hardware firewall?

Most individual home users 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.

Email Safety

Following some simple guidelines can help you safeguard your email environment. Email is often used to transport malware and broadcast phishing scams.

Malware
Email commonly transports malware (malicious software) that can result in identity fraud or computer damage. Malware describes any program designed to cause harm. Some common types of malware include viruses, worms and trojans.

Phishing
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 such as passwords or financial data.

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 for fraud.

Never open or respond to SPAM (unsolicited bulk mail 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 the 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 extensions.
Most files use filename extensions such as ".doc" for documents or ".jpg" for images. If a file has a double extension, like "heythere.doc.pif" it is 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 if opened.

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

Online Identity Protection

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

Be selective about where you surf.
Not all Web sites 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 (a Web page is secure if there is a locked padlock in the lower left-hand corner of your browser).

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 choose "Remember My Password."
You should never use the "remember password" feature for online banking or transactional Web sites.

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, shut down.
Always sign off from online banking or any other Web site 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.

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.

Lock your mailbox.
Preferably, your personal mailbox should lock. Don't leave mail in your mailbox longer than necessary – especially if your mailbox does not 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 out 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 and 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.

Online Banking Tips

- Navigant Credit Union will never email or call you to ask for your Online Banking USER ID or Password.
- When enrolling in Enhanced Login Security, choose to receive your temporary pass code by telephone or text message, it's the most secure!
- Periodically change your online banking password (at least every 90 days)
- Report any suspicious activity during your online banking session to the Online Banking Department at Navigant Credit Union.
- Click the "Logout" button when you have finished your online banking session. Closing the browser webpage by clicking "X" does not end your session properly.
- If you are accessing your account through a mobile device, be sure to use passcode or biometric protection on the device to prevent unauthorized access.