Why isn’t “more” better?

Maybe there is an extra software program included with a program you bought. Or perhaps you found a free download online. You may be tempted to install the programs just because you can, or because you think you might use them later. However, even if the source and the software are legitimate, there may be hidden risks. And if other people use your computer, there are additional risks.

These risks become especially important if you use your computer to manage your personal finances (banking, taxes, online bill payment, etc.), store sensitive personal data, or perform work-related activities away from the office. However, there are steps you can take to protect yourself.

How can you protect both your personal and work-related data?

Use and maintain anti-virus software and a firewall – Protect yourself against viruses and Trojan horses that may steal or modify the data on your own computer and leave you vulnerable by using anti-virus software and a firewall. Make sure to keep your virus definitions up to date.

Regularly scan your computer for spyware – Spyware or adware hidden in software programs may affect the performance of your computer and give attackers access to your data. Use a legitimate anti-spyware program to scan your computer and remove any of these files. Many anti-virus products have incorporated spyware detection.

Keep software up to date – Install software patches so that attackers cannot take advantage of known problems or vulnerabilities. Many operating systems offer automatic updates. If this option is available, you should turn it on.

Evaluate your software’s settings – The default settings of most software enable all available functionality. However, attackers may be able to take advantage of this functionality to access your computer. It is especially important to check the settings for software that connects to the internet (browsers, email clients, etc.). Apply the highest level of security available that still gives you the functionality you need.

Avoid unused software programs – Do not clutter your computer with unnecessary software programs. If you have programs on your computer that you do not use, consider uninstalling them. In addition to consuming system resources, these programs may contain vulnerabilities that, if not patched, may allow an attacker to access your computer.

Consider creating separate user accounts – If there are other people using your computer, you may be worried that someone else may accidentally access, modify, and/or delete your files. Most operating systems (including Windows XP and Vista, Mac OS X, and Linux) give you the option of creating a different user account for each user, and you can set the amount of access and privileges for each account. You may also choose to have separate accounts for your work and personal purposes. While this approach will not completely isolate each area, it does offer some additional protection. However, it will not protect your computer against vulnerabilities that give an attacker administrative privileges. Ideally, you will have separate computers for work and personal use; this will offer a different type of protection.

Establish guidelines for computer use – If there are multiple people using your computer, especially children, make sure they understand how to use the computer and internet safely. Setting boundaries and guidelines will help to protect your data.

Use passwords and encrypt sensitive files – Passwords and other security features add layers of protection if used appropriately. By encrypting files, you ensure that unauthorized people can’t view data even if they can physically access it. You may also want to consider options for full disk encryption, which prevents a thief from even starting your laptop without a passphrase. When you use encryption, it is important to remember your passwords and passphrases; if you forget or lose them, you may lose your data.

Follow corporate policies for handling and storing work-related information – If you use your computer for work-related purposes, make sure to follow any corporate policies for handling and storing the information. These policies were likely established to protect proprietary information and customer data, as well as to protect you and the company from liability. Even if it is not explicitly stated in your corporate policy, you should avoid allowing other people, including family members, to use a computer that contains corporate data.

Dispose of sensitive information properly – Simply deleting a file does not completely erase it. To ensure that an attacker cannot access these files, make sure that you adequately erase sensitive files.

Follow good security habits – Review other security tips for ways to protect yourself and your data.
How do you know if your privacy is being protected?

Privacy policy – Before submitting your name, email address, or other personal information on a website, look for the site’s privacy policy. This policy should state how the information will be used and whether or not the information will be distributed to other organizations. Companies sometimes share information with partner vendors who offer related products or may offer options to subscribe to particular mailing lists. Look for indications that you are being added to mailing lists by default—failing to deselect those options may lead to unwanted spam. If you cannot find a privacy policy on a website, consider contacting the company to inquire about the policy before you submit personal information, or find an alternate site. Privacy policies sometimes change, so you may want to review them periodically.

Evidence that your information is being encrypted – To prevent attackers from stealing your personal information, online submissions should be encrypted so that it can only be read by the appropriate recipient. Many sites use Secure Sockets Layer (SSL) or Hypertext Transport Protocol Secure (https). A lock icon in the bottom right corner of the window indicates that your information will be encrypted. (See Understanding Web Site Certificates for more information.) Some sites also indicate whether the data is encrypted when it is stored. If data is encrypted in transit but stored insecurely, an attacker who is able to break into the vendor’s system could access your personal information.

What additional steps can you take to protect your privacy?

Do business with credible companies – Before supplying any information online, consider the answers to the following questions: Do you trust the business? Is it an established organization with a credible reputation? Does the information on the site suggest that there is a concern for the privacy of user information? Is legitimate contact information provided? If you answered “No” to any of these questions, avoid doing business online with these companies.

Do not use your primary email address in online submissions – Submitting your email address could result in spam. If you do not want your primary email account flooded with unwanted messages, consider opening an additional email account for use online. Make sure to log in to the account on a regular basis in case the vendor sends information about changes to policies.

Avoid submitting credit card information online – Some companies offer a phone number you can use to provide your credit card information. Although this does not guarantee that the information will not be compromised, it eliminates the possibility that attackers will be able to hijack it during the submission process.

Devote one credit card to online purchases – To minimize the potential damage of an attacker gaining access to your credit card information, consider opening a credit card account for use only online. Keep a minimum credit line on the account to limit the amount of charges an attacker can accumulate.

Avoid using debit cards for online purchases – Credit cards usually offer some protection against identity theft and may limit the monetary amount you will be responsible for paying. Debit cards, however, do not offer that protection. Because the charges are immediately deducted from your account, an attacker who obtains your account information may empty your bank account before you even realize it.

Take advantage of options to limit exposure of private information – Default options on certain websites may be chosen for convenience, not for security. For example, avoid allowing a website to remember your password. If your password is stored, your profile and any account information you have provided on that site is readily available if an attacker gains access to your computer. Also, evaluate your settings on websites used for social networking. The nature of those sites is to share information, but you can restrict access to limit who can see what.

Author
US-CERT Publications
What is a social engineering attack?
In a social engineering attack, an attacker uses human interaction (social skills) to obtain or compromise information about an organization or its computer systems. An attacker may seem unassuming and respectable, possibly claiming to be a new employee, repair person, or researcher and even offering credentials to support that identity. However, by asking questions, he or she may be able to piece together enough information to infiltrate an organization’s network. If an attacker is not able to gather enough information from one source, he or she may contact another source within the same organization and rely on the information from the first source to add to his or her credibility.

What is a phishing attack?
Phishing is a form of social engineering. Phishing attacks use email or malicious websites to solicit personal information by posing as a trustworthy organization. For example, an attacker may send email seemingly from a reputable credit card company or financial institution that requests account information, often suggesting that there is a problem. When users respond with the requested information, attackers can use it to gain access to the accounts.

Phishing attacks may also appear to come from other types of organizations, such as charities. Attackers often take advantage of current events and certain times of the year, such as

- natural disasters (e.g., Hurricane Katrina, Indonesian tsunami)
- epidemics and health scares (e.g., H1N1)
- economic concerns (e.g., IRS scams)
- major political elections
- holidays

How do you avoid being a victim?
Be suspicious of unsolicited phone calls, visits, or email messages from individuals asking about employees or other internal information. If an unknown individual claims to be from a legitimate organization, try to verify his or her identity directly with the company.
Do not provide personal information or information about your organization, including its structure or networks, unless you are certain of a person’s authority to have the information.
Do not reveal personal or financial information in email, and do not respond to email solicitations for this information. This includes following links sent in email.
Don’t send sensitive information over the Internet before checking a website’s security.
Pay attention to the URL of a website. Malicious websites may look identical to a legitimate site, but the URL may use a variation in spelling or a different domain (e.g., .com vs. .net).
If you are unsure whether an email request is legitimate, try to verify it by contacting the company directly. Do not use contact information provided on a website connected to the request; instead, check previous statements for contact information. Information about known phishing attacks is also available online from groups such as the Anti-Phishing Working Group.
Install and maintain anti-virus software, firewalls, and email filters to reduce some of this traffic.
Take advantage of any anti-phishing features offered by your email client and web browser.

What do you do if you think you are a victim?
If you believe you might have revealed sensitive information about your organization, report it to the appropriate people within the organization, including network administrators. They can be alert for any suspicious or unusual activity.
If you believe your financial accounts may be compromised, contact your financial institution immediately and close any accounts that may have been compromised. Watch for any unexplainable charges to your account.
Immediately change any passwords you might have revealed. If you used the same password for multiple resources, make sure to change it for each account, and do not use that password in the future.
Watch for other signs of identity theft.
Consider reporting the attack to the police, and file a report with the Federal Trade Commission.

Author
US-CERT Publications
Is identity theft just a problem for people who submit information online?

You can be a victim of identity theft even if you never use a computer. Malicious people may be able to obtain personal information (such as credit card numbers, phone numbers, account numbers, and addresses) by stealing your wallet, overhearing a phone conversation, rummaging through your trash (a practice known as dumpster diving), or picking up a receipt at a restaurant that has your account number on it. If a thief has enough information, he or she may be able to impersonate you to purchase items, open new accounts, or apply for loans.

The Internet has made it easier for thieves to obtain personal and financial data. Most companies and other institutions store information about their clients in databases; if a thief can access that database, he or she can obtain information about many people at once rather than focus on one person at a time. The Internet has also made it easier for thieves to sell or trade the information, making it more difficult for law enforcement to identify and apprehend the criminals.

How are victims of online identity theft chosen?

Identity theft is usually a crime of opportunity, so you may be victimized simply because your information is available. Thieves may target customers of certain companies for a variety of reasons; for example, a company database is easily accessible, the demographics of the customers are appealing, or there is a market for specific information. If your information is stored in a database that is compromised, you may become a victim of identity theft.

Are there ways to avoid being a victim?

Unfortunately, there is no way to guarantee that you will not be a victim of online identity theft. However, there are ways to minimize your risk:

- Do business with reputable companies – Before providing any personal or financial information, make sure that you are interacting with a reputable, established company. Some attackers may try to trick you by creating malicious web sites that appear to be legitimate, so you should verify the legitimacy before supplying any information. Take advantage of security features – Passwords and other security features add layers of protection if used appropriately. Check privacy policies – Take precautions when providing information, and make sure to check published privacy policies to see how a company will use or distribute your information. Many companies allow customers to request that their information not be shared with other companies; you should be able to locate the details in your account literature or by contacting the company directly.
- Be careful what information you publicize – Attackers may be able to piece together information from a variety of sources. Avoid posting personal data in public forums. Use and maintain anti-virus software and a firewall – Protect yourself against viruses and Trojan horses that may steal or modify the data on your own computer and leave you vulnerable by using anti-virus software and a firewall. Make sure to keep your virus definitions up to date.
- Be aware of your account activity – Pay attention to your statements, and check your credit report yearly. You are entitled to a free copy of your credit report from each of the main credit reporting companies once every twelve months.

How do you know if your identity has been stolen?

Companies have different policies for notifying customers when they discover that someone has accessed a customer database. However, you should be aware of changes in your normal account activity. The following are examples of changes that could indicate that someone has accessed your information:

- unusual or unexplainable charges on your bills
- phone calls or bills for accounts, products, or services that you do not have
- failure to receive regular bills or mail
- new, strange accounts appearing on your credit report
- unexpected denial of your credit card

What can you do if you suspect or know that your identity has been stolen?

Recovering from identity theft can be a long, stressful, and potentially costly process. Many credit card companies have adopted policies that try to minimize the amount of money you are liable for, but the implications can extend beyond your existing accounts. To minimize the extent of the damage, take action as soon as possible:

- Start by visiting IdentityTheft.gov – This is a trusted, one-stop resource to help you report and recover from identity theft. Information provided here includes checklists, sample letters, and links to other resources.
- Possible next steps in the process – You may need to contact credit reporting agencies or companies where you have accounts, file police or other official reports, and consider other information that may have been compromised.