

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. Some sites also indicate whether the data is encrypted when it is stored. If data is encrypted in transit but stored non-securely, 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.

Authors

CISA