

Internet Security Best Practices

We at Illinois National Bank want to provide some recommendations to help prevent some of the common fraudulent activities that occur on the Internet including phishing, pharming and other scams that can lead to identity theft.

Anti-Virus

- Install and/or update antivirus software.
- Update antivirus signatures on a regular basis. Running updates once a day is recommended since new viruses and exploits are released daily.
- Run a virus scan of all of your files on a weekly basis. Most AV vendors use a scanning engine that actively scans files that are being used by you or your operating system. Running a weekly "Full Scan," will help catch any malicious software that may not be actively in use.

Personal Firewall

- Install and/or update firewall software. There are many commercially available programs that package both anti-virus and personal firewall software together. Personal firewalls can help keep hackers from directly installing software on your PC and can alert you if a program you did not install is trying to access the internet.
- If an intrusion detection engine is part of your firewall program, regularly update intrusion detection signatures.

Anti-Spyware

- Install and/or update anti-spyware software. Anti-spyware software also helps keep unwanted software off of your PC and can also detect software that may have been installed without your knowledge.
- Update anti-spyware signatures on a regular basis.
- Run a spyware scan of all of your files on a weekly basis. Most anti-spyware vendors use a scanning engine that actively scans files that are being used by you or your operating system and prevents certain unwanted modifications from occurring. Running a weekly "Full Scan," will help catch any malicious software that may not be actively in use.

Patch Management

- Keeping your operating system and browser up to date is one of the easiest methods of keeping your computer safe on the internet.
- Periodically check your operating system's vendor for updates. Since the majority of home PC's run a version of Microsoft's Windows operating system, we have included the link for Microsoft's Windows Update [here](#).

Browsing Habits

- If you are on a site that asks for personal information (social security number, account number, credit card number, etc.) check for the following on the web page:

- Make sure the web address starts with https://
- Look for a closed lock either by the address or down in the bottom frame of your browser. If that lock is missing, the page is not encrypted and your information can be seen as it passes across the internet.
- Some browsers and the new version of Internet Explorer (version 7) that will be released soon, use a color coding in the address bar to let you know if the page is properly secured. Web pages use certificates to encrypt your data. Most use red as a page with a bad certificate and green to let you know that the certificate is valid. An address bar that is white in a browser that supports the color coding does not have a certificate. The current versions of Internet Explorer do not use this color coding even if the page is secured properly. Check with your browser vendor to find out the color coding used.
- Another good habit is to type the address of the page you are browsing in the address bar instead of following a link. Links can be spoofed to look valid but may take you to another site without your knowledge. Favorites can also be hijacked and altered to take you to the site that you did not intend to visit.
- Never write down usernames and passwords. If you do, make sure that they can be secured in a locked drawer. The most common place that passwords are found is on monitors, under keyboards and mouse pads, and in desk drawers.
- Make sure that your password is something that is easily remembered by you alone. Using combinations of uppercase and lowercase letters, numbers, and “special characters” is recommended. Special characters are symbols like @, %, \$, and !. Changing your password will also make it harder for hackers or other people to guess your password.