Do you know all the ways your identity is at risk online?

There are many ways your personal information can be at risk online:

1. Spyware and Malware can record your keystrokes to gain personal information.
2. Careless use of public computers or wireless networks can expose your personal information to strangers.
3. Seemingly innocent posts and status updates can provide clues to your habits that criminals can exploit.
4. Fraudulent emails and job offers lure people into providing sensitive information to criminals.

What can you do to protect your personal information online?

A few simple changes in the way you think about and use the Internet can go a long way toward reducing or eliminating the risk that your personal information can be used fraudulently by criminals.

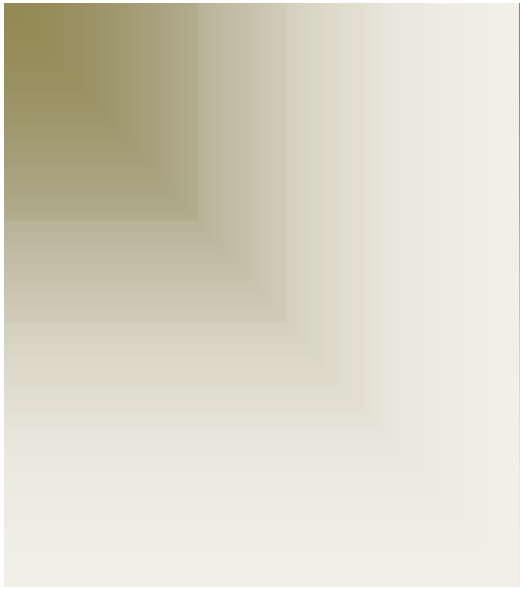
Best Practices for Online Security

Local County Public Library
Some street
Some town, ST 12345
Phone: 555-555-5555
Fax: 555-444-4444

www.yourlibrary.com

Best Practices for Online Security

and preventing identity theft.



Avoid Spyware, Malware, and Viruses

These are malicious programs that infect your computer through the Internet. These programs can not only harm your computer, but can record keystrokes, capturing credit card numbers, bank account numbers, and social security numbers and relaying them back, over the internet, to someone else. Even if you never enter this information into a Website, malicious programs can find this information if you have it stored on your computer. Here are some steps you can take to avoid infecting your computer with these programs:

1. Avoid downloading programs from disreputable sites.

2. Don't click on any pop-up advertisements. Though they may look reputable, it is difficult for the average user to know where they originated.

3. Use an antivirus program along side of spyware and malware scanners, and keep them updated. A good source of information on how to do this is http://www.securitytango.com

Keep these things in mind when working on public computers and wireless networks

1. Use a firewall to ensure others can't access your computer through an unsecured network. Password protecting directories can also keep others out of your files.

2. Remember to log out of accounts such as email, social networking sites, and shopping sites when you are finished with a public computer. If you forget, the next person who goes to gmail or facebook may find they are logged into your account.

3. Be aware that auto-fill features in internet browsers can retain log-in information, addresses, credit card and bank account numbers. This information is then automatically entered into those fields the next time someone visits the same site on the same computer you used. Save shopping and banking for computers that you know no one else will access.

Don't reveal too much information about yourself online.

1. Don't reveal your real name (especially if it's unusual), your location, or other information that might allow others to identify you. A name and a town or the name of a school might be enough for a stranger to track down your address.

2. Information about vacations or daily plans can signal to thieves that you won't be at home.

3. Pictures of cars and houses can reveal license plates and house numbers.

4. Only do business on reputable sites that encrypt personal information.

5. Nothing on the Internet ever disappears. 20 years from now embarrassing information could come back to haunt you. Employers, lawyers, and peers could make use of information that you thought harmless at the time.

Fraudulent Communications

There are many types of fraudulent email that can leave you vulnerable to fraud.

1. It sounds like it should be obvious, but any unsolicited request for you to deposit a large sum of money on someone else's behalf is fraudulent. Do not reply to these requests.

2. Likewise, unsolicited job offers requesting personal information such as social security numbers are fraudulent. Especially if the offer is for a job that is not in your field, it is best not to reply to these emails, or be very cautious with your reply.

3. Criminals can hack into instant messaging accounts or social networking accounts pretending to be someone you know. They claim to be stranded in a foreign country and ask that you wire money immediately.

Avoid all of these types of fraudulent communications.

1. Don't open email from someone you don't know.

2. Check out any urgent requests for money that are made over the internet from people you do know.

Many people believe their identities are safe online. However, due to lack of information, they leave themselves vulnerable to identity theft through risky online behavior. Reputable sites encrypt personal information to keep it from being accessed by thieves. Read and understand the privacy policies of the sites you visit to have better control of the information about you that's out there. Avoid communication from people you don't know and be careful about the sites you visit, what you download, and how you access the Internet in public. These few changes can improve your online safety.