Computer Safety Tips

1. Use Appropriate Security Settings On Social Media

On all social media websites, like Facebook, there are security settings that can be adjusted to give you the level of privacy you want. You can adjust who can and who cannot see the things you post, your profile picture, or your personal information like your address, birthday, and email. Any personal information you choose to put on your social media can be accessed by anyone unless you change these settings on your account. You can adjust privacy settings by going to your account settings, or you can ask a trusted friend or family member for help.

2. Log Out Of Your Accounts When You Are Finished Using Them

Staying logged into an account can put your information at risk of being exposed to someone who should not have access to it. If you log into a bank account, social media account, or other online account that contains sensitive information, be sure to log off once you have finished using it.

3. Never Save Your Login Information To A Computer

Many websites allow you to save your login information, so you do not have to remember a username and password each time you log in. This can be helpful if you have difficulty remembering your login information. However, if anyone else is able to access the device or computer with the saved login information, then they will be able to access any sensitive information within your accounts.

4. Install Antivirus Software On Your Computer

Installing antivirus software and keeping it up to date can prevent viruses and spyware from infecting your computer. This protects valuable information that may be stored on your computer such as login information to your bank accounts.

5. Learn to Spot and Avoid Online Scams

Some scams are easy to spot and easy to avoid. It can get tricky to spot a scam when it comes from a profile, private message, or email from a friend. Scammers can duplicate or hack into profiles and emails and send you messages soliciting personal information or money. If you are concerned a message might be coming from a scammer and not from the friend who allegedly sent you the message, call and talk to the friend directly. Also, avoid clicking on ads and materials that pop up on your computer screen. For more information on scams, visit our pages on Personal Safety and Security and Scams & Fraud.

6. Never Give Out Personal Information

Never post personal information like addresses or phone numbers on social media or other sites. You may receive a request from someone claiming to be a government agency like the Social Security Administration. Do not give your personal information to these people.

7. Just Because It Is On The Internet Does Not Mean It Is True

Everybody has the ability to post information on the internet, so a lot of the information you find may not be true. It is important that you look at the sources the information comes from and check that it is a trusted source. You should always look at the author or entity publishing the information, look to the date to see how relevant the information is, and look to the domain name.

8. Talk To Someone You Trust

If you are unsure about whether something you have seen online or have been asked to participate in is a scam, talk to a trusted family member or friend. Some websites, online stores, or social media pages may seem safe to use but may really be a scam or otherwise be dangerous to use. If you are unsure about anything you are doing or have been asked to do online, talk to someone you trust about whether it is a

good idea.

Last updated on March 27, 2024.

Print

Table of Contents

NEWS

News & publications

The news about recent activities for needed peoples.

[More News](#)

26 Apr 2022

Chat Bots for Family Law, Landlord-Tenant, and Workers Compensation

Need Legal Help? Check Out Our Chat Bots! We currently have three…

[Continue Reading](#)

14 Apr 2022

Free Senior Legal Helpline

Are you a senior citizen with legal questions? If you're 60 or older…

[Continue Reading](#)

Our Partners

Our Partners