General Safety Tips

1. When using a computer that is not your own, personal device, ALWAYS log out of websites when you are done! If you do not, the next person to use that computer could have access to your account and your personal information.
2. Do your updates! The updates often contain fixes for new security issues.
3. Lock your device! Take the time to create a code and set a timer to lock your screen so that if your device is lost, no one can access your information. Do not use your birthdate or other number series that are public information
4. Be cautious on public networks! Avoid accessing private information on a public Wi-Fi. Make sure the network you choose is the one you want. Thieves will name Wi-Fi options "Free Public Wi-Fi" to gain access to your information.

"I read it on the internet, it must be true!"

-No one, ever

Evaluate Your Online Sources:

Who: What are the qualifications of the author? Do They have a biased view they are trying to present?

What: What information is presented? What information is missing?

Where: What kind of Website is this? Blog? Do they have an agenda they are promoting?

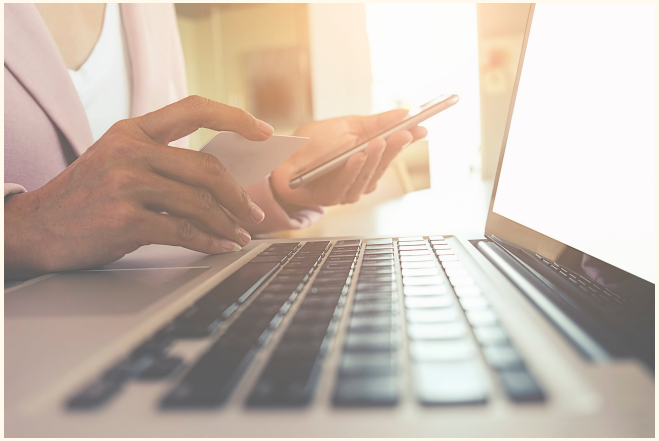
When: How old is the information?

Make our community **Internet Smart**! Share these tips with your family and friends.

BANDERA PUBLIC LIBRARY

Protect Yourself!

Safety Tips for Internet Use



Use this guide to help make your internet experiences safer and more enjoyable.

Protect Yourself

Passwords: Many websites require you to make an account and password for your protection when using their services. You need to choose something that is:

1. Memorable: use a phrase that you will easily remember.
2. A Mix of letters and numbers and symbols. Mix these in logical places, like ! in place of I or $ in place of S.
3. Never use a word spelled out in it's normal manner. This is very easy for professionals to decode.

Example of a good password:

Using that phrase "You Are My Sunshine" mixed with the digits of an address: Y7A2M0$0

Phishing and Scams

For internet criminals, the main focus is to get your personal information any way they can.

BEWARE:

- Apps that do not come from an official app store. The can have phishing software attached that can steal your personal information.
- Emails that ask for your password, personal information or credit card information. Your bank, credit card company, etc. will NEVER ask for this by email. Always go to the actual website for the business that has contacted you and contact them that way, rather than replying to an email.
- Make sure that the web address begins with HTTPS: and that there is a closed lock in the address bar before putting in your information. This shows that the site is secure.
- The phrase" If it looks too good to be true, it probably is." should be applied to any "great deal" you may be offered.
- Never, ever send money to anyone that you are not positive that you know who they are. If in doubt, use a pay service such as PayPal, to protect your money.
- Never give your personal information to anyone unless you are positive that you know exactly who they are. Passwords and account information should never be shared without verification of who it is being shared with.

Be Aware!

Criminals work hard to make emails and websites look legitimate just to steal your information. Be AWARE and look for signs that something may be wrong. Protecting your information now can save you a lot of money and time later.