Digital Safety

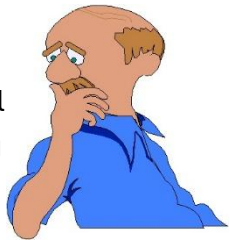
August 28, 2025

You won't find the following information online, it represents information collected over the years by the authors. It's not a guarantee that you won't be hacked, but it provides a lot of useful information for your use and to protect you.

Safety used to be the domain of physical security, ensuring the safety of property and family. Lately, digital safety has become more of a concern as society is more integrated and predators roam the web. This document attempts to address some of those concerns and better prepare our membership for using the web. As an introductory note, it's always a good idea to backup your data to the cloud or a jump drive in case your computer crashes, or if someone has penetrated your armor and is holding your computer hostage for ransom. And if you keep a password file, please encrypt the data.

Most Windows desktop computers have Windows Defender to protect your browsing and email experience, other platforms may have Norton Antivirus, McAfee and other software. Make sure the virus definitions and software are up to date and maintained.

If you're concerned about someone stealing your identity, the best approach to protect yourself is to freeze your credit at the 3 main credit agencies, i.e. Equifax, Transunion and Experian. Banks will not issue a credit card or extend credit to an unauthorized individual when your credit is frozen, and it's relatively easy; and it can be temporarily undone if you need a car loan, open a new bank account, etc. More information may be found at https://www.usa.gov/credit-freeze.



Email/phone calls

Information for the majority of people is usually readily available on the web. For example, https://clustrmaps.com/ has name, address, email, phone number, date of birth and other information, and https://voterrecords.com has similar information. The point being, you may get a phone call or email from someone pretending to be someone they're not. Although flyers may show contact information for committee chairs, the Parrotheads will never disclose your phone number, email or other information.

If you get any unsolicited phone calls, ask if you can call them back if they start asking personal questions - then call them on the phone number you have in your directory for their business. If you get a phone call or email message saying your computer is infected with a virus, it is NOT. Hang up the phone call, delete the email message. Hackers are quite prolific in using this tactic to prey on unsuspecting users. If you get an unsolicited email, do NOT click on anything in the email as it's likely a phishing message (not to be confused with the Parrotheads) trying to get you to bite. If you get an email and your

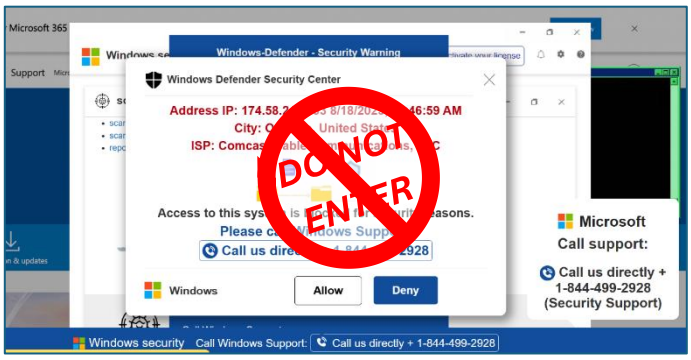
antivirus pops up saying an attachment is infected, delete the email and notify the sender that they sent you an infected file. If you suspect an email is not from a friend, click on the from field and observe the physical email address. Hackers will generate an obscure email address to avoid being caught, so it's probably spam if the from field looks like a lot of gibberish. If you're interested in the subject area, Google the subject area and approach the website in a manner you trust, analogous to going in the front door of a business's website.

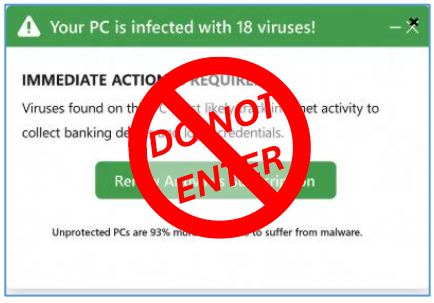
Websurfing

When going to a website, those beginning with "https://" are encrypted and secure where those beginning with "http://" are not. This is not an issue per-se, but don't share personal data on a website beginning with "http://". Also, any website with a "####.gov" extension such as "https://www.usa.gov/" mentioned above is usually associated with a government agency and is relatively safe.

One Parrothead asked if he should invest in virtual private network (VPN). The author used VPN for work purposes before retiring, for logging into sensitive business systems. VPN is used at a hotel or other location where the Wifi isn't secure so that anyone monitoring your browsing activity only see encrypted communications (i.e. gibberish). VPN encrypts data as does "https://", but won't encrypt text messages sent from your phone through the cloud. So it's somewhat of a personal decision to invest in VPN - web data is encrypted using "https://" but email isn't.

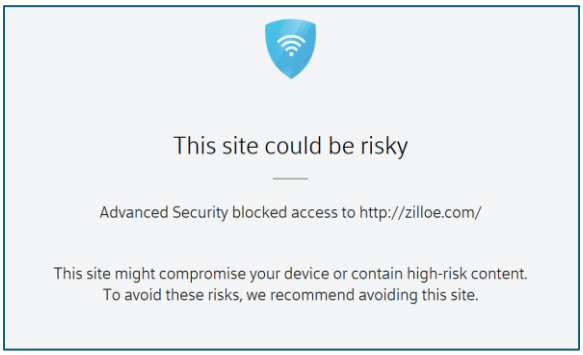
When looking at websites, hackers may "hijack" your web browser with a window saying you have a virus or have to update your virus definitions. Clicking anywhere on the window doesn't seem to work as they hijacked your browser. Below is an example of the window that results. If you get this, don't panic and do NOT click on anything – simply turn your computer off and on again.





When surfing the web using a browser, be mindful of nefarious websites that are seeking your information to steal your identity. Never give out your name, address and other personal information unless you're sure the website is legitimate. Ask yourself, why do they need this information, and is it necessary?

Lastly, if you're going to a webpage and wind up somewhere that looks suspect, check the spelling of the website. Hackers will buy a domain that's similar to but a little off the main website. For example, if you want to go to Zillow and inadvertently type Zilloe.com (vice Zillow.com, easy to do), you are redirected to a suspect website. The following window pops up in Windows Defender, but the cell phone takes you to the site. Don't click on anything, just correct the spelling of the website in the address bar.



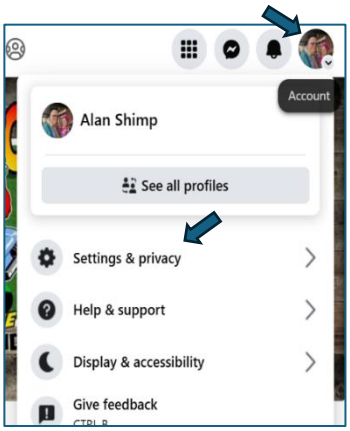
Facebook

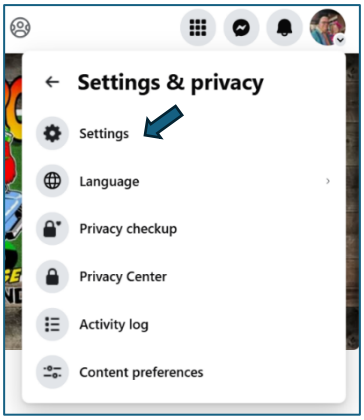
It was noted that some of our members had their Facebook profile cloned, i.e. hacked by nefarious individuals, and invites sent out to all their friends. The default for Facebook is for a member's Friends List to be visible to everyone, i.e. the list is "public". Essentially, a nefarious person would copy someone's profile picture, set up a new Facebook profile with the same name and picture, and send friend requests out to everyone - pretending to be the Parrothead being cloned. To protect against this, below are detailed instructions for changing who can access your Friends List from "public" to "friends". If the nefarious individuals don't have access to your Friends List, it's unlikely they'll be bothered to clone you. We strive to make your web browsing experience a little easier and safer.

Digital Safety

August 28, 2025

On your Facebook page, click on your icon (or ≡ on a cell phone) in the upper right and then “Settings & privacy”. On the screen that follows, click on “Settings”





This brings up the settings menu for Facebook. Scroll down to “Audience and visibility”, and click on “How people find and contact you”. Click on “Who can see your friends list?” and change it from “Public” to “Friends”. Click “Done”, or “Save” on a cell phone.