Tips and Tricks for Safe-Surfin' the Social Media Waves
July 13, 2026 Quick Bytes

1. Spoofed emails
    a. If you hover your mouse over the "from email address", it can reveal the true email. Same with any links in the email. Best practice, never click on links sent in emails unless you can strongly verify who it is from and that it is a valid link.
    b. Never open a zip folder sent to you without some verification of who set it to you.
2. Passwords and IDs to accounts should be a mix of alpha/numeric/character/symbols. Never use phrases, names, etc., even with the symbols/numbers, etc.
    a. Password Generator: https://randompasswordgenerator.com/. A software tool (app) that automatically creates strong, random, and unpredictable passwords. It's safe to use.
    b. You can set the parameters for the type of password that will fit the account, not all of them will allow the various symbols that are shown. You can edit those, removing the ones not accepted by the account.
3. Use "Have I been Pawned" to check your emails and passwords. https://haveibeenpwnd.com/.

4. Setting up 2FA (2 factor authentication).
    a. You can use an Authenticator App. Google and Microsoft make them. Not all sites will be set up for this, check the security settings.
    b. Set up for SMS codes to be sent or have them sent to a general email.
    c. Set up the use of a Windows Passkey. If that is a selection, when you click on that it will bring up the Windows Passkey, the same one you have set up to sign into your computer. You can set it for a set of four numbers or mix it alpha/numeric, again, make it random.

5. Facebook and other social media accounts, directories, etc.
    a. Cloning and hacking are two very different events. Your profiles can be cloned. If your profile is set to "public", it is easy for bad actors to harvest your information and create another profile of you; name, photos, location, education, etc.
        i. Check the Security & Privacy settings
        Click your picture in the upper right-hand corner
        Click Settings & Privacy
        Click Privacy
            Review all those settings, ensure you have the most privacy.
            You can set it so only those that are friends or friends of friends can view your full profile. This keeps "scrappers" from pulling pics, personal information, etc. from your account.

ii. Go back and click on Settings.
    - Review the side bar, you can use the search for a particular setting.
    - Search for 2FA, click Two-factor authentication and set it up.

iii. Go back, search for Profile: Review the settings there as well

6. Best Practices:
    a. Always use complicated passwords. Where permitted use complicated IDs for signing into all accounts, not just financial.
    b. Change passwords over 90 days max; over 30 days if you believe you have been hacked.
    c. When you change the password to one account, review all accounts connected to that one account and change those passwords as well. It is a chain effect.
    d. Create a spreadsheet. Easy way is one column for the link to the website where you log in. Another column is your log in ID. The next column is the password. Next one for notes: Security questions and answers. Last column is the date the password was changed.

"Hacking" means an unauthorized person has broken into your actual computer, device, or account to steal or manipulate data. They may use methods like malware, phishing links, or brute-force password guessing. Your accounts are compromised, may lose access and you might notice changed passwords or unauthorized sent messages. Bad deal. Change all passwords, run antivirus scans.

"Spoofing" however, means the attacker didn't touch your device at all; they simply impersonated your identity (like your email address or phone number) to trick others. It's a disguise trick. Your device and accounts are safe, and because your account isn't compromised, changing your password won't stop a spoofer. Report the impersonation to the platform—Instagram or Facebook help center. And let people know it wasn't you.