CYBER JAGROOKTA DIVAS – SEPTEMBER 2022
FIRST WEDNESDAY OF EVERY MONTH

CYBER CAUTION:
ONLINE SAFETY TIPS

Tip #1: Know the dangers of the internet

When it comes to cybersecurity, kids are often one of your family's weakest links — and that can be for lack of knowing the dangers of the internet. Teach kids about suspicious activity online and encourage them to ask for help if something seems unusual.

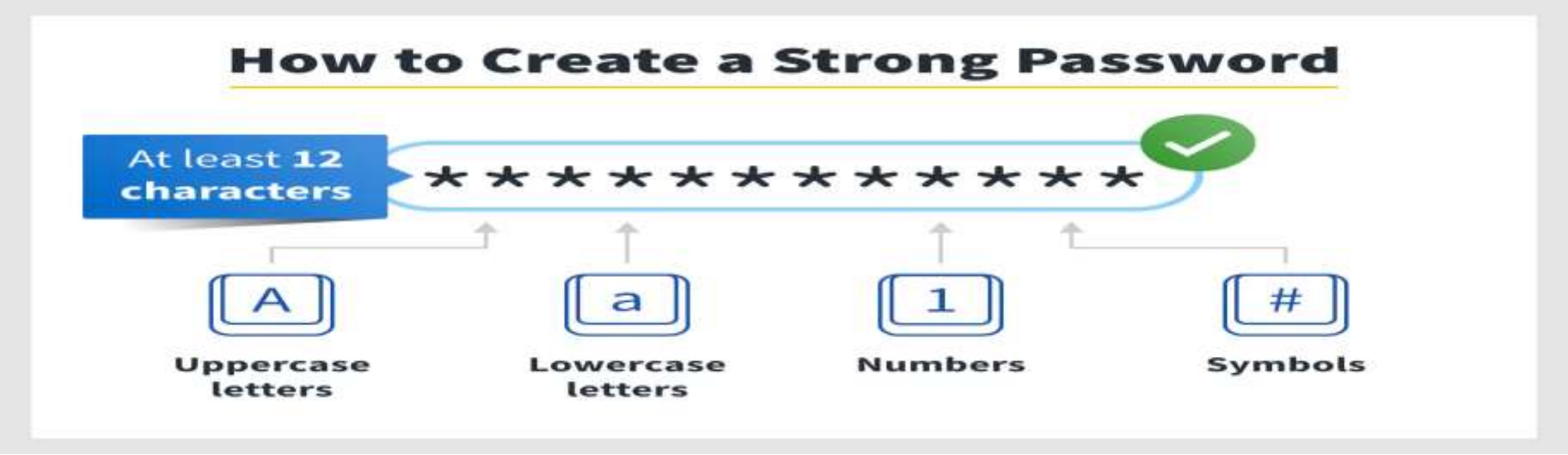
Tip #2: Remember your identity is important

Sometimes kids make themselves vulnerable to identity theft by disclosing personal information online because they believe they have nothing to lose. A child's identity can have as much value as an adult's identity, if not more. Scammers can trick kids into disclosing their Social Security number and other details that can be used to commit identity theft. Remind children not to reveal too much information about themselves. Their date of birth, address, and SSN are all examples of personal information, and they shouldn't share them freely.

Tip #3: Beware of strangers

Offline, you've probably already introduced the idea to your kids that all strangers can be potentially dangerous. Remind them this also applies to their online activities and strangers are on the internet. While teens may be more prone to advances from online predators, kids can be targeted, as well. It's important to teach them at a young age to be cautious online and tell an adult if someone they don't know communicates with them or makes them uncomfortable.

Tip #4: Choose strong passwords



Passwords are the primary defense against hackers. Yet, many people reuse the same password for multiple accounts and use passwords that are easy to guess, because they're also easy to remember. Teach your kids to create a hack-proof password by selecting a combination of uppercase and lowercase letters, numbers, and symbols, and make sure it's at least 12 characters long. Never use common words, phrases, or personal information like a phone number or family members' names.

Tip #5: Keep your social media accounts secure

There's a good chance someone in your house is on a social network. But social media can also attract cyber snoops and identity thieves. Keep a close eye on your social accounts. If someone messages you who hasn't done so in a while, be suspicious. Your friend's account may have been hacked. Parents should remind teens to also never meet in person with someone they met online and tell an adult if a stranger is messaging them.

Tip #6: Be careful what you post

It's important for children, teens, and family members to know how much information is too much information. In their excitement to share milestones, teens may sometimes post their personal information online. For example, a driver's license or a travel itinerary shared online could be valuable information for identity thieves or burglars. Also personal or inappropriate photos can attract online predators, or could affect future educational or employment opportunities.

Tip #7: Understand privacy policies …

With more websites and applications collecting information and using it for advertising and marketing purposes, make sure your family knows the value of online privacy. Many apps have privacy policies that disclose that the apps collect and share their users' information. Kids and many adults often accept these policies without reading them. Even if your settings are set to private, remember nothing is private. Even the so-called private browser is not private. Law enforcement, website administrators, and hackers could have access to your so-called private information.

Tip #8: Backup data regularly

A type of malware, ransomware is popular among cybercriminals who can lock your computer so you can't access your valuable files, like your private photos or tax information. One of the best ways to combat the threat of ransomware is to backup your data regularly. Backup your kids' devices, too, and teach your teens to do the same.

Tip #9: Go private on public Wi-Fi

There are a lot of risks of connecting to public Wi-Fi networks. In addition to keeping your kids and teens attuned to them, it's important for parents to remind themselves that hackers and cybercriminals consider public Wi-Fi, such as in malls and coffee shops, an easy access point to getting hold of your data. For this reason, always use a VPN when connecting to public Wi-Fi. Don't have a VPN? Consider if you can hold off on internet browsing until you are home.