School's out for summer!

Kids Internet Safety

Our kids are out of school for the summer, soaking up the sun, but they will probably be soaking up some of the Internet, too. We would like to assume our kids know how to use the internet safely, but that is not always the case. This month's newsletter will highlight tips that will help keep your kids safe while online.

1. Keep personal information private.

Remind kids that we should never share things like our addresses, phone numbers, pictures of ourselves, email addresses, or even school names should not be shared.

2. Be extra careful when interacting with strangers online

Often, many of the games that kids play are online and games that connect them with people worldwide.

If kids have online friends, all we know about them is what they tell us, which might not be who they really are. It is crucial for kids to keep these interactions short and not share too many details about themselves.

3. Keep passwords private

Kids should never share their passwords with anyone besides their parents or guardians. Doing this will help keep their accounts and their information safe.

4. Be open to talking about what they are doing online. Make it a regular thing!

Having conversations about what they are doing online and what they like to browse, watch or play will allow them to feel comfortable when an issue arises and they need to talk to a trusted adult about what is going on.

5. Be cautious of what is clicked on or downloaded.

The internet is full of things to click on. Take time to show your kids how to inspect links online. Show them how to hover the mouse over a link and where the URL pops up. You can talk about the difference between .com, .org, .gov etc.

Have them review with an adult before they download anything. Sometimes, viruses are hidden behind downloads that could harm computers or tablets.

Keep it updated!

You may or may not have noticed, but updates to popular systems like Google Chrome, Apple iOS, Android, and more have been rolling out over the last month. Updates to systems are to help patch any vulnerabilities. A vulnerability is "a weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source."

Turn on automatic update settings on your phone and computer to ensure that you are up to date with the latest system versions; this will prompt you to update on time and keep you and your devices safe.

Phishing in the summer

Hackers are trying to catch employees off guard while we all relax a little now that summer is upon us! With more employees working from home or on vacation, people might not take the time to think critically about the links they are clicking on or what Wi-Fi they are using. Continue to use best practices when reading emails and joining public Wi-Fi.