INFORMATION SECURITY TEAM MESSAGE:
Top ten cybersecurity Tips for summer

With summer approaching, our thoughts turn to sunny days, BBQ's, and vacations. But before the fun begins, let's take a moment to make sure we and those we care for are safe. At USFHP, we strive to ensure your data is safe; we want to make sure you are safe as well.

Here are our top ten cybersecurity tips to make sure your summer is safe and enjoyable.

1. Protect all your smart phones and tablets with a PIN or password. If your phone is lost or stolen, this will be the only thing keeping others locked out from the contents of your phone.
2. Before going on any trips make sure your smartphone is backed up. Vacations are always something to look forward to, but as fun as they are they can be hectic. Make sure your smart devices are backed up before you go to avoid any accidents that may occur.
3. Don't advertise your whereabouts to hackers! Turn off auto-location and check-in apps when you travel to avoid being an easy target. Try to avoid checking into locations and turn off the location settings on your photos. Post all your amazing photos once you get home.
4. Only connect to Wi-Fi that is password protected and avoid checking bank accounts or shopping on any public Wi-Fi, even if it is password protected. It's tempting to always be connected, but make sure the connection is secure.
5. Turn off Wi-FI, Bluetooth, and location services if you're not using them. Not only will it save your battery, but it will also further protect you from anyone nearby trying to get into your device.
6. Avoid talking about anything personal around "always on devices." Protecting your privacy today is a challenge, and with devices listening for key phrases to activate, the challenge increases.
7. Consider using a password manager. While traveling you may need to create multiple accounts for different places to use their services. Instead of using the same username and password, consider letting a password manager handle it for you.
8. When traveling, avoid using auto-connect or disable it. Most rental cars and hotels feature auto-connect experiences. If you have to connect your smartphone or other smart device using auto-connect, disable it once done to avoid exposing your device to intruders.
9. Check your privacy settings on social media and other public accounts. Social media lets us connect with anyone, anywhere, anytime, but be sure to visit the privacy settings for each site to make sure you're sharing only with the people you want to. Avoid announcing to potential burglars that you are on vacation and only share with your friends and family.
10. Consider using two-factor authentication for all services and accounts that offer it. Two-factor authentication is one of the best ways to protect any account. Use it to stop keep hackers from accessing your devices even if they know your password.

We here at the USFHP Information Security Team hope you have a most excellent, safe, healthy, and happy summer.

USFHP at PacMed Information Security Team

Don Carter
Information Security Manager

McCall Paxton
Senior Information Security Engineer

Abolaji Filani
Information Security Analyst