DigiKnow

CYBER SECURITY DEPENDS ON YOU

SUMMER IS HERE

Summer is for family fun, festivals and food. As we move into July and August, many families hit the road for vacation. This issue we offer suggestions for being safe online particularly when traveling. We highlight information pertaining to kids and teens, many of whom may have less supervision and spend more time online. Please take a few moments to enjoy a safe cyber summer.

— Solomon Adote, Chief Security Officer.

Tech Travel Tips

Password protect all your devices.

Enable multi-factor authentication for important applications such as email and cloud storage services. This can prevent unauthorized access to confidential information.

Make sure your applications and antivirus software are up to date *before you leave*.

If possible, install a firewall: give your device an added layer of protection against unauthorized access.

Limit password attempts: some devices allow you to choose the number of password attempts. Others have an option that erases all data if the password is entered incorrectly 10 times. Enable these options so that if you lose the device, that's all you'll lose.

Gotcha tools: Learn how to enable any available anti-theft measures on your devices, like remote locking, wiping, and/or tracking.

Disable wireless (WiFi) connections when you don't need your device to connect to the Internet.

Bring your USB charger power plug: don't plug your device's USB cord into a strange device's USB port! Merely plugging in makes you susceptible to malicious software downloads – you don't even have to click on anything to be infected.

A mass AirDrop could descend upon your iPhone this summer. *The Atlantic* magazine explored this phenomena, so popular among teens and tweens. While most AirDrops are funny memes, they can also be bullying and inappropriate.

AirDrop, an instant file-sharing feature on Apple devices, lets users send photos, videos, contacts, links, and more via a combination of Bluetooth and WiFi. Total strangers with AirDrop enabled can share files from up to 30 feet away. Used irresponsibly, it can create trouble.

How? In a crowd of people—enough so it's not immediately clear who sent it—teens start dropping photos, memes, selfies, and more to every AirDrop receptive device around. Teens often edit the identity of their iPhone or iPad to something anonymous or funny to compound the joke.

Naturally, some people push the boundaries of acceptability. It's not unheard of for kids to blast out pornographic images (of themselves or others). Bullying one another by distributing compromising or unflattering classmate photos is another problem. AirDrop is automatically enabled on every Apple device and transmissions are not traceable. Since it is not a social media app, there are no moderation or reporting tools, nor are there adverse consequences such as being banned, as might happen on Instagram, for instance.

Luckily, AirDrop allows you to control what your device receives. Bring up the Control Center Below the playback controls you'll see "AirDrop;" On some devices, you may need to go to Settings/General/ Airdrop. You can change from the default of receiving AirDrops from "Everyone" which makes you vulnerable. Select from the other available options the one that makes sense for you: **Turn it off** completely or accept AirDrops from "**Contacts Onl**y" to only receive AirDrops from people already listed in your device's contacts.

Questions, comments or topic suggestions? Email us at eSecurity@delaware.gov

DEPARTMENT OF TECHNOLOGY & INFORMATION
DELIVERING TECHNOLOGY THAT INNOVATES

Delaware Department of Technology and Information publishes and sends this newsletter to all network users because we need YOUR help to keep our network secure. If you are having problems viewing this message, accessing the links, or want to print a PDF copy, go to https://digiknow.dti.delaware.gov.