What is Juice Jacking?

Tuesday, November 23, 2021

YOU SHOULD BE WARY OF USING COMMUNAL PHONE CHARGING STATIONS FEATURING USB OUTLETS.

Hey Wildcats!

I'd like to briefly introduce myself as this is my first blog post for SHARPP (yay!). My name is Ava Courduvelis and I am currently a junior here at UNH. I am majoring in neuroscience and behavior as well as minoring in Spanish. This is now my second semester being a part of SHARPP. Last semester my role in SHARPP was a community educator. At SHARPP, community educators contribute to outreach and education for the UNH community by focusing on interpersonal violence prevention. This semester, I have taken on an additional role at SHARPP. I am now also the new

marketing and communications assistant! What this means is that you will see me on here posting new blog posts every now and then.

Now that I have introduced myself, let's dive into what I wanted to talk about for this post. I'll start off by asking a question – have you ever seen communal phone chargers at your local mall, airport or even in your Uber? Now for a follow-up question – have you ever used one of those chargers? If you answered "yes" to the follow-up question, you may want to continue reading to find out why that may not be such a good idea.

Imagine this: You are out in public and your phone has very low battery. You want to be able to check your texts, Snapchat your friend back and watch the daily Tik Tok or two that your roommate sends you. How can you possibly do all those things when your phone is about to die? Well, you can't, at least not for long. So, the only thing you can do is avoid using your phone. Bummer. We all know that takes a lot of self-control to do. Suddenly, you notice free charging stations right in front of you. What a miracle! Wrong. You probably shouldn't use it ... a simple plug-in to that charger may cause irreversible breaching of your personal data. This is what is known as juice jacking.

One may ask, "how could a USB steal my information?" The answer is actually quite simple. A hacker will first use a USB to place malware (malicious software) designed to hack your device onto a public charging station. Then, when you plug your device in to the charging kiosk you become vulnerable to the hacking as you are directly connected to it by a USB. Two things could happen when you connect your device. First, your personal information such as banking numbers, photos, passwords and more could be stolen through the USB and sucked into the hacker's hub. The second thing that could happen is that malware could be installed onto your device. If malware is installed onto your device, then even after you unplug it, it is still being compromised. Your location, calls and texts could be monitored in real time by the hacker. There is even malware that can clone the data from your device onto another device, meaning that the hacker could even try to impersonate you. It is important to know that a USB cable is more than a charger, as it is also used to sync data. This is what makes everything mentioned possible.

So how do you know if a charging station will juice jack you? The short answer is you can't tell. However, if while using the charger you notice that your phone starts opening pop-ups or starts being controlled on its own, you should unplug your phone immediately as that is a sign you may be being juice jacked. Definitely unplug your phone if you ever get a notification asking to "Trust this computer?" That one speaks for itself.

While this is a lot of alarming information, there are preventative measures that we can all take to make sure we do not fall victim to juice jacking. It is important to be informed and prepared for such a situation. First and foremost, the easiest way to avoid juice jacking is to bring your own personal charger with you and make sure to plug it into an outlet (NOT a USB port). This is the most reliable preventative measure. Another option is to bring a portable charger with you. There are also phone cases that charge your phone, which allows for longer lasting battery. Now, if you still really want to connect to a USB port there is an option for you. USB condoms exist! What in the world is a USB

condom, you may ask? Well, they are also known as juice jack defenders, and they are adaptors that block the data transfer pins of a USB. With these, you can still charge your device, but data exchange will be blocked. If you want to go even further, there is also anti-virus protection available for installation. Lastly, a good thing to do is to always update your phone when an update is available. The software update notifications are pretty annoying, I know, but when better and more secure software is available, why not take it, right?

The time for holiday traveling is approaching, so remember to avoid the charging stations at the airports or rest stops you may be at. Make sure to educate your friends and family about juice jacking. Stay safe everyone and see ya' next blog post!

- WRITTEN BY:
  Ava Courduvelis | SHARPP Student Marketing and Communications Assistant

SEXUAL ASSAULT EDUCATION AND PREVENTION

University of New Hampshire

UNH Today is produced for the UNH community and for friends of UNH.
The stories are written by the staff of UNH Communications and Public Affairs.
Email us: unhtoday.editor@unh.edu.

MANAGE YOUR SUBSCRIPTION **CONTACT US**

Like us on Facebook

Follow us on Twitter

Follow us on YouTube

Follow us on Instagram

Find us on LinkIn

UNH Today RSS feeds

UNH Today • UNH Main Directory: 603-862-1234
Copyright © 2022 • TTY Users: 7-1-1 or 800-735-2964 (Relay NH)
USNH Privacy Policies • USNH Terms of Use • ADA Acknowledgement