What’s New?

Summer is in full swing! While you’re on vacation, that doesn’t stop attackers from deploying their schemes. In this newsletter, we are going to cover the highlights of malware recently discovered on Android devices, recent innovations in phishing, and review the nature of the latest viral phenomenon, FaceApp.

Agent Smith

Are you an Android user that has been getting more popup ads than ever before? This is likely due to recently detected malware called Agent Smith. When downloaded, the malware disguises itself as legitimate Google updating tools. The best action to protect against this attack is to update your phone with the latest security patches, refrain from clicking any ads, and to stay away from any unofficial Android app stores.

Microsoft OneNote Audio Note Phishing Campaign

Attackers who send out phishing campaigns are adapting their ways. A recent campaign claims you have a Microsoft OneNote Audio Note message from a contact in your address book. When you click on the "Listen to full message here" link, you will be brought to a fake OneNote Online page hosted on Sharepoint.com, the webpage, currently disabled, would prompt the target to enter their Microsoft login credentials. If you have received this email, be sure to Report as Phishing and forward it to the IT_Security_Team@grcc.edu.

Gone Viral: FaceApp

Similar to the discovery with Cambridge Analytica collecting and selling user data by way of personality quizzes, now pops up FaceApp. It started like many viral trends, with celebrities, as seen above with the Jonas Brothers, posting seemingly accurate photos of themselves aged.

What you need to know is simple: Users of FaceApp grant the Russian parent company of the app the rights to do anything they would like with the images they upload. The company, Wireless Lab, publicly stated that “images are deleted within 48 hours of upload but are temporarily stored on American servers”. However, the terms and conditions can be changed at any time and without notice.

The key is to be aware of who you are providing your information to. It’s all fun and games until someone hurts/compromises the information you’ve provided to the company that doesn’t keep your information safe and secure.