# Cyber Roundup – November 2022

By Thomas J. DeMayo, Principal, Cybersecurity and Privacy Advisory

To minimize your risk of downloading and installing a malicious app, while not foolproof, here are a few things you can do to protect yourself.

- Determine if the creator is a legitimate company.
- Ensure that the app's request for your access information matches the functions it is to provide. For instance, if requesting the app for Google maps, it makes sense that you will need to provide your location. On the other hand, if you want to download an app that teaches your young children the alphabet, such a request for your location would be suspicious.
- Find out how long the app has been in existence. If the app has been functional for multiple years, is widely used, matured in versions, etc., it is likely less risky than a brand-new app from an unknown developer.

## Key Cyber Events

The following is a rundown of trends and what's been happening recently in the cyber world. We welcome your comments, insights and questions.

- **In research from Netacea, refund-as-a-service fraud is up 60% in cybercriminal forums.** Refund fraud takes advantage of store return policies. Fraudulent claims may be made that an order never arrived, claiming to send an order back while keeping the product, claiming parts are missing, etc. In a refund-as-a-service model, fraudsters are hired to utilize their social engineering skills, often in combination with the use of third-party services to generate fake tracking and return information. In exchange, the fraudster will receive a portion of the profit.
- **United States airport websites suffered a denial-of-service attack from a pro-Russian cybercriminal group, dubbed Killnet.** The airports restored operations in short order. While the attacks did not cause any harm, they did result in disruptions. In addition, the media attention garnered by the attack may inspire other groups to launch similar attacks against other critical infrastructures.
- **Meta, the parent company of Facebook, alerted that over 400 malicious iOS and Android apps had been identified on the respective app stores designed to steal Facebook credentials**. The apps ranged from photo editors, games, VPN services, among others. Credentials of approximately 1 million users may have been compromised as a result of the apps.
- **The FTC targeted the homework help application, Chegg, for what it called "careless" cybersecurity.** The app exposed the details of approximately 40 million users. Sensitive data, such as student's sexual orientation, disabilities, religion and family income were exposed. One of the issues noted was the excessive assignment of administrative (full) access to employees and contractors.

  ***Tom's takeaway:*** Permissions, permissions, permissions. One of the top issues we find in our assessments is excessive permission assignment. This often results from the simplicity of granting more instead of less, and/or, not having a process in place to reverify and readjust permissions over time. When attackers gain access, they often gain access under the context of the user account on the machine or application they impacted. The more users with excessive access, the more opportunities they have to exploit that data in some fashion. Take the time to ensure all users are only granted access to what they need and nothing more.

- **A research team identified that Thomson Reuters exposed approximately three terabytes of sensitive information as a result of a misconfiguration.** That misconfiguration left three of its databases exposed to the public internet. The Company immediately fixed the issue upon notification and launched a detailed analysis to determine the cause of the incident. Impacted customers are being notified.

- **Following is a summary of Ransomware events in October:**

  - The fourth largest health care system, CommonSpirit, suffered a ransomware attack that resulted in delayed surgeries and the disruption of patient care as key systems needed to be taken offline to deal with the incident. Almost a month after the attack as of this writing, the system is still trying to fully restore operations and bring their patient care systems back online. The system is working with forensic investigators to help determine if patient data was breached as a result of the attack.

  - The Indianapolis Housing Agency suffered a major ransomware attack that compromised its entire IT environment. The attack disrupted the ability of the agency to send out October rent checks for the 8,000 families that depend on them. The attack, which occurred in early October remained ongoing through the month, as the agency's IT service providers, law enforcement and incident responders attempted to regain control.

  - Medibank, an Australian health insurer, suffered a ransomware attack that resulted in the unauthorized access of 9.7 million individuals. Compromised data consisted of such identifying information as name, address, birthdate, phone, email, passport information, etc. In addition, health claims data on approximately 500,000 individuals was taken. The Company refused to pay the ransom. The ransomware gang behind the attack, REvil, has since begun to release the information to their dark web site.

    ***Tom's takeaway:*** I typically focus on U.S. based issues; however, it is important that we don't lose sight that the cyber threat is a global issue. We are all in this together and need to appreciate that our actions or inactions as they relate to cybersecurity have implications much greater than ourselves.

## Contact Us

Thomas J. DeMayo, CISSP, CISA, CIPP/US, CRISC, CEH, CHFI, CCFE
Principal
Cybersecurity and Privacy Advisory
tdemayo@pkfod.com | 646.449.6353

Nick DeLena, CISSP, CISA, CRISC, CDPSE
Partner
Cybersecurity and Privacy Advisory
ndelena@pkfod.com | 781.937.5191