



UCF Information Security Office

David Zambri
Associate Vice President and Chief Information Security Officer

Top 3: Security News in June 2024

- Accidental or Not, Another Google Leak Exposes Multiple Privacy Breaches**
[CyberNews.com](#)
An internal Google database was just leaked anonymously to 404 Media, an online news outlet, and it showed huge issues with privacy and security at the company.
- Ticketmaster Breach Confirmed, Third Party Blamed**
[CyberNews.com](#)
On May 20th, Live Nation “identified unauthorized activity within a third-party cloud database environment containing Company data (primarily from its Ticketmaster L.L.C. subsidiary),” the filing with the SEC reads.
- Celebrity TikTok Accounts Compromised Using Zero-Click Attack via DMs**
[TheHackerNews.com](#)
Popular video-sharing platform TikTok has acknowledged a security issue that has been exploited by threat actors to take control of high-profile accounts on the platform.

DID YOU KNOW?



NSA Warns iPhone & Android Users to Restart Devices Once Every Week

According to the NSA, restarting mobile devices can help disrupt the operations of malware and other malicious software that may have infiltrated the system.

[Click to read more.](#)



Research discovers the 25 most hacked pop culture passwords

By analyzing more than 300 million exposed passwords from the Pwned database, the research determined the top 25 hacked passwords from pop culture.

[Click to read more.](#)



83% of organizations faced at least one account takeover the past year

Furthermore, 45.5% of organizations experienced more than five account takeover incidents in the past year, and nearly one in five experienced more than 10. [Click to read more.](#)

Summer Cybersecurity: Think Before You Click

As June ushers in the start of summer, bringing with it warm weather and vacation plans, it's an excellent time to remind ourselves of the importance of cybersecurity. While we relax and enjoy the season, cyber threats don't take a holiday. This month, let's focus on a crucial aspect of digital safety: mindful clicking.

Mindful Clicks: Navigating the Internet City

Imagine the internet as a sprawling, bustling city with countless doors leading to different places. Your clicks are the keys that open these doors. Just as you wouldn't open random doors in an unfamiliar city, exercise the same caution online. Every click has the potential to lead you to safe, well-known destinations or into the risky alleys of cyber threats.

The Golden Rule: Stay on Well-Lit Streets

When browsing online, stick to well-known, well-lit internet streets—trusted websites and sources. These sites are like your favorite neighborhood spots, familiar and reliable. Avoid venturing into mysterious, unmarked websites that promise too much but could deliver harm. Think of trusted sources as your safe havens in the vast digital city.

Email Caution: Handle with Care

Emails often come with attachments and links, akin to receiving packages and letters. Treat these with caution. Before clicking on an email link or opening an attachment, verify the source. Is it from someone you know? Were you expecting this email? Cyber attackers frequently use phishing tactics, disguising malicious content as legitimate communication.

Cyber Bodyguards: Protecting Your Online World

Think of cybersecurity tools as your personal bodyguards in the digital world. These tools help you filter out suspicious content and prevent malicious code from entering your system. They provide an additional layer of protection, ensuring that only safe and trusted elements are allowed through. Keeping these digital bodyguards active and up-to-date is essential for maintaining a secure online environment.

Think Before You Click: Your Guide to Safe Computing

Adopting a mindful approach to clicking is like having a seasoned guide in the digital city, steering you towards safe and secure paths. This summer, as you enjoy the freedom and relaxation of the season, remember to think before you click. A moment's hesitation can prevent a world of trouble.

Stay safe online this June, and let mindful clicks lead you to a secure and enjoyable summer!

In Other (Security) News...

» **Infosec2024 Spyware: A Threat to Civil Society and a Threat to Business**

Commercial spyware poses a threat to enterprises as well as individuals and civil society, according to an expert panel at Infosecurity Europe 2024.

[Click to read more.](#)

» **New PyPI Malware “Pytoileur” Steals Crypto and Evades Detection**

The package, posing as an “API Management tool written in Python,” concealed code that downloads and installs trojanized Windows binaries. These binaries are capable of surveillance, achieving persistence and stealing cryptocurrency. The package was discovered by Sonatype's automated malware detection systems and quickly taken down after being flagged. [Click to read more.](#)

» **Account Takeovers Outpace Ransomware as Top Security Concern**

A recent survey conducted by Abnormal Security has spotlighted account takeover attacks as the foremost threat facing today's organizations. According to the company's 2024 State of Cloud Account Takeover Attacks report, 83% of organizations experienced at least one account takeover in the past year.

[Click to read more.](#)

Security Alerts



» **Google released fixes for a high-severity security flaw in Chrome that has been actively exploited**

[Click to read more.](#)

» **Memory corruption issue for older iPhone and iPads**

[Click to read more.](#)