مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Apple ID Push Bombing Scam Campaign

Tracking #:432315736

Date:29-03-2024

EXECUTIVE SUMMARY:

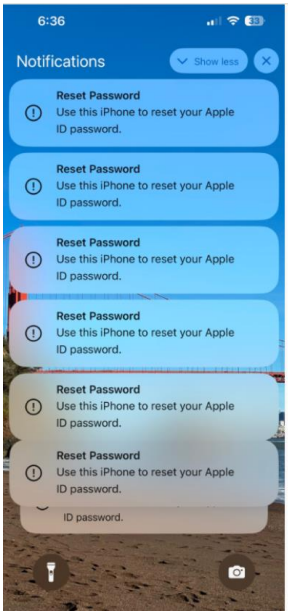
The UAE Cyber Security Council has observed a recent Apple ID phishing campaign has targeted tech professionals, including startup founders and cybersecurity experts.

TECHNICAL DETAILS:

A recent Apple ID phishing campaign has targeted tech professionals, including startup founders and cybersecurity experts. Attackers utilize "push bombing" tactics, bombarding victims' devices with password reset prompts, and caller ID spoofing to impersonate Apple Support. This strategy aims to pressure victims into unknowingly granting access to their Apple ID and potentially compromising sensitive data.

Impacts:
Account Takeover: Attackers could gain access to the victim's iCloud account.
Data Breach: Attackers could access sensitive photos, notes, files.
Remote Device Wipe: Scammers could remotely wipe the victim's devices using "Find My."
Disruption and Productivity Loss: The sheer volume of notifications can be overwhelming and disrupt normal device usage.
Targets: Tech professionals, startup founders, cybersecurity experts

Attack Methods:
Push Bombing: Attackers trigger hundreds of Apple ID password reset prompts on victims' devices.
Caller ID Spoofing: Scammers impersonate Apple Support via phone calls with a spoofed caller ID to trick victims into revealing one-time passwords (OTPs)
Personal Information Harvesting: Attackers may use personal information obtained from "people search" sites to appear legitimate.



RECOMMENDATIONS:

- Don't Panic During Push Bombing: Carefully review notifications before clicking "Allow."
- Enable Two-Factor Authentication: This adds an extra layer of security beyond your password.
- Be Wary of Unsolicited Calls: Never provide OTPs or other sensitive information to unknown callers, even if they claim to be from Apple Support.
- Scrub Your Data: Consider removing your information from "people search" sites to limit access to personal details.
- Stay Vigilant: Be aware of phishing tactics and avoid accidental misclicks due to the overwhelming nature of push bombing.
- Report Phishing Attempts: Report suspicious activity directly to Apple.

REFERENCES:

1. https://krebsonsecurity.com/2024/03/recent-mfa-bombing-attacks-targeting-apple-users/