**If you (and I) are using an i-phone in public especially on public transportation, criminals are trying to watch our keystrokes to steal our passcodes, then grab our i-phones, and exit public transportation, then access our bank accounts. When I am on our local bus or mass transit train, almost everyone is using their cell phone.**

Even though Face Recognition is secure for now, if criminals can steal your passcode, and then grab your cell phone, they can use the stolen passcode to change the pass code so that they can control your iPhone and drain your bank account (s) before you can stop them. Thieves have even tried to capture the keystrokes for passcodes by using their iPhone or other cell phone cameras. (Not easy do, especially if you block your screen so that no one can see your keystrokes.)

Key Defense, i-phone users must never allow anyone to grab their phone and run. The thieves will attempt to capture your passcode, if you key in your passcode in public. If you must use your passcode in public, make sure no one is looking over your shoulder, or sitting next to you. They will scout for easy victims like seniors, or ladies.

Many of the thieves are young men, so they are likely stronger than their victims. In public transportation, it is not unusual to see i-phone users hanging on the a strap or an overhead, or side bar, and holding with one hand, the i-phone. It doesn't take a lot of strength to just grab your i-phone, and dash away.

For the thief, they would like to grab the i-phone when the bus, or is stopped so that they can make a quick exit. And the victim may not have even seen the face of the thief.

**====================================================**

**Source:**

**Criminal Use IPhones to Steal Digital Lives.**

**Passcode Interception Exploits Security Flaw**

**Joanna Stern, Nicole Nguyen, *WSJ*, Feb 25-26, 2023, A1, A11**

NEW YORK—In the early hours of Thanksgiving weekend, Reyhan Ayas was leaving a bar in Midtown Manhattan when a man she had just met snatched her iPhone 13 Pro Max.

Within a few minutes, the 31-year-old, a senior economist at a workforce intelligence startup, could no longer get into her Apple account and all the stuff attached to it, including photos, contacts and notes. Over the next 24 hours, she said, about $10,000 vanished from her bank account.

Similar stories are piling up in police stations around the country. Using a remarkably low-tech trick, thieves watch iPhone owners tap their passcodes, then steal their targets’ phones—and their digital lives.

The thieves are exploiting a simple vulnerability in the software design of over one billion iPhones active globally. It centers on the pass-code , the short string of numbers that grants access to a device; and passwords, generally longer alphanumeric combinations that serve as the logins for different accounts.

With only the iPhone and its passcode, an interloper can within seconds change the password associated with the iPhone owner’s Apple ID. This would lock the victim out of their account, which includes anything stored in iCloud. The thief can also often loot the phone’s financial apps since the pass-code can unlock access to all the device’s stored passwords.

“Once you get into the phone, it’s like a treasure box,” said Alex Argiro, who investigated a high-profile theft ring as a New York Police Department detective before retiring.

He said there have been hundreds of these sorts of crimes in the city in the past two years. “This is growing,” he said. “It is such an opportunistic crime. Everyone has financial apps.”

Apple Inc. has marketed itself as the leader in digital privacy and security, selling its tightly integrated hardware, software and iCloud web services as the best protection for its customers’ data. “Security researchers agree that iPhone is the most secure consumer mobile device, and we work tirelessly every day to protect all our users from new and emerging threats,” an Apple spokeswoman said.

“We sympathize with users who have had this experience and we take all attacks on our users very seriously, no matter how rare,” she said, adding that the company believes these crimes are uncommon because they require the theft of the device and the passcode. “We will continue to advance the protections to help keep user accounts secure.”

An examination of the recent spate of thefts reveals a possible gap in Apple’s armor. The company’s defenses are designed around common attack scenarios—the hacker on the internet attempting to use a person’s login credentials, or the thief on the street looking to snatch an iPhone for a quick sale.

**Prowling bars**

They don’t necessarily account for the fog of a late-night bar scene full of young people, where predators befriend their victims and maneuver them into revealing their passcodes. Once thieves possess both passcode and phone, they can exploit a feature Apple intentionally designed as a convenience: allowing forgetful customers to use their passcode to reset the Apple account password.

“It was only a matter of time before an attacker would use shoulder surfing or social engineering,” said Adam Aviv, an associate professor of computer science at George Washington University. Relying on a phone as a trusted device fails in such cases, he added.

All of the victims interviewed by The Wall Street Journal said their iPhones were stolen while they were out at night socializing. Some said the phones were grabbed out of their hands by someone they had just met. Others said they were physically assaulted and intimidated into handing over their phones and pass-codes. A few said they believe they were drugged. They woke up the next morning missing their phones, with no memory of the previous night.

In all cases, the iPhone owners were locked out of their Apple accounts. They then discovered thousands of dollars in financial thefts, including some combination of Apple Pay charges, drained bank accounts linked to phone apps and money taken from PayPal Holdings Inc.’s Venmo and other money-sending apps.

A similar vulnerability exists in Google’s Android mobile operating system. However, the higher resale value of iPhones makes them a far more common target, according to law-enforcement officials. “Our sign-in and account-recovery policies try to strike a balance between allowing legitimate users to retain access to their accounts in real-world scenarios and keeping the bad actors out,” a Google spokesman said.

On the evening of Jan. 22, 2022, Reece Thompson, an art director at a creative agency in Hiawatha, Iowa, was having a drink with his girlfriend while visiting downtown Minneapolis when his iPhone 12 Pro went missing from the bar. The next morning, when he tried to log into his Apple account from a different device, the account password had been changed. Thousands of dollars had been charged to his credit cards via Apple Pay and $1,500 was stolen from his Venmo account, he said.

**Minneapolis ring**

Minnesota prosecutors say Mr. Thompson, age 42, was a victim of a theft ring that accumulated nearly $300,000 by stealing iPhones and their passcodes from at least 40 victims. The group targeted bar-goers with Apple smartphones, quickly looted accounts accessible via those devices and then resold the phones, according to the arrest warrant for one member of the alleged ring, Alfonze Stuckey. Mr. Stuckey has since pleaded guilty to one count of racketeering and received a 57month prison sentence. Eleven other suspects have been charged with racketeering in the case.

Mr. Stuckey, 23, who has a previous record of misdemeanors, said he wouldn’t comment unless he is compensated. His lawyer declined to comment.

Groups of two or three thieves would go to a bar and befriend victims, often asking them to open up Snapchat or some other social-media platform, said Sgt. Robert Illetschko, the lead investigator on the case. During that interaction they would try to observe the victim unlocking the iPhone with the passcode, he said. If they didn’t catch the passcode at first, they might have tried to get the victim to hand them the phone for a photo and then subtly turn it off before handing it back, he added. After an iPhone is restarted, a passcode is required to unlock it.

“It’s just as simple as watching this person repeatedly punch their passcode into the phone,” said Sgt. Illetschko, adding that sometimes thieves would covertly film victims so they could be sure they caught the correct sequence. “There’s a lot of tricks to get the person to enter the code.”

Similar cases have been reported in Austin, Denver, Boston and London.

In New York City, one of the first inklings police received about the extent of this new crime wave came in the form of an unexplained death.

On Friday, May 27, while visiting from Washington, D.C., John Umberger went out for the night in Manhattan, ending the evening at a bar in the Hell’s Kitchen neighborhood. Five days later the 33-year-old director of diplomacy and political programs at the American Center for Law and Justice was found dead in the apartment he was staying in, with an emptied wallet and no iPhone.

At first, police suspected it was a routine drug overdose. Then his family discovered thousands of dollars had been taken from his bank, PayPal and Venmo accounts, along with suspicious credit-card charges, according to Mr. Umberger’s mother, Linda Clary. She believes her son’s Apple account password was changed.

Mr. Argiro, the New York City detective who participated in the investigation of Mr. Umberger’s death before retiring in September, said authorities came to believe he was the victim of a group of thieves that target New York bar-goers, launder money via apps and then resell the phones. This particular group is believed to be responsible for more than 30 incidents, he added.

The Manhattan district attorney’s office is assembling a case to present before a grand jury, according to people familiar with the investigation.

**The method**

In theory, recent security innovations from Apple should eliminate the vulnerability of an intercepted passcode. The Apple spokeswoman pointed to Face ID and Touch ID as ways that would limit the need to type a passcode at all.

Yet in New York, some authorities have suggested Face ID as a possible point of entry into the phones. The city’s Office of Nightlife, a liaison between City Hall and the hospitality industry, hosted a speaker who recommended bar-goers disable facial recognition, on the theory that an incapacitated person’s face could be used by the thieves.

A passcode breach is the more likely scenario, according to the Journal’s reporting and on-device testing. To change someone’s Apple ID password on an iPhone, a face scan won’t suffice: A passcode is needed. When the password change is complete, the software offers an option to force other Apple devices, such as Macs or iPads, to sign out of the Apple account, so a victim couldn’t turn to those devices to regain access. The software never requires the user to enter an older password before setting a new one. Journal reporters were able to do all that in less than a minute.

An Apple spokeswoman said the system is designed to help users who have forgotten their account password. She added that it requires two factors, the physical device as well as the device’s passcode.

**Find My iPhone**

With the new password, the thief can disable Find My iPhone, which would otherwise allow victims to locate their phones and even remotely erase them to protect their data. Disabling Find My iPhone also allows the thief to resell the iPhone.

Apple recently introduced the ability to use hardware security keys, little USB dongles, to protect the Apple ID. In the Journal’s testing, security keys didn’t prevent account changes using only the passcode, and the passcode could even be used to remove security keys from the account.

Taylor Ashy, a sales executive at a New York-based tech company, said he was drugged the night of Dec. 10, 2021, at a New York bar. He has no recollection of how his phone was taken. All he knows is that whoever took it gained access to his bank app, enrolled his bank’s debit card in Apple Pay, and opened a Venmo credit card and Apple credit card in his name.

Mr. Ashy, who had more than $10,000 transferred out of his bank account, said he stored passwords to those accounts in Apple’s iCloud Keychain password manager. The feature auto-fills login information following successful Face ID or Touch ID scans, or the input of the iPhone’s pass-code, according to the Journal’s testing. In Mr. Ashy’s case and others, the bank fraud happened after the victims’ biometrics were no longer available to the thieves.

If apps require text-message codes as part of their logins, a security practice known as two-factor authentication, the messages are sent to the iPhone—the same one a thief would be holding.

After logging into bank apps with the passcode, the Journal was able to add digital debit cards to Apple Pay without needing the physical cards or their PINs. Money can be sent from the debit cards to Apple Cash, which can be used to send money or to make con-tactless payments at stores.

Several victims said an Apple credit card was opened in their name. The cards quickly accrued thousands of dollars in charges. Accessed through Apple’s Wallet app, an Apple Card application will autofill with information that might be stored on the iPhone, such as the owner’s name, address and birthday.

The Apple Card form does require applicants to enter the last four digits of their Social Security numbers. One victim, David Vigilante, believes the thieves found that information right in the Photos app on his iPhone XS Max.

After having the phone stolen at a pizza shop on Manhattan’s Lower East Side in the early hours of Oct. 23, the 30year-old product manager at a real-estate data company realized someone had attempted to charge $15,000 to his credit card via Apple Pay and that a new Apple credit card had been opened in his name. When he got back into his Apple account a few days later, he found photos he had previously taken of sensitive documents— his passport, driver’s license, paycheck direct-deposit form and health-insurance paperwork—collected in a new photo album.

Apps such as Apple Photos, iCloud Drive and Google Drive now offer the ability to search text within images and documents. In the Journal’s tests, a search in the Apple Photos app for “SSN” (Social Security number) and “TIN” (taxpayer identification number) immediately produced a photo of a 1099 tax form with Social Security information that had been stored on the phone.

Some people whose iPhones were stolen are unable to regain access to their Apple accounts. With the passcode, an Apple ID’s backup email and phone number can be changed, and a security feature called a recovery key can be enabled. In recent cases, thieves changed the Apple account’s contact information and turned on the recovery key, blocking victims from being able to use an account-recovery service for those who forget their Apple ID password.

The Apple spokeswoman said that account-recovery policies are in place to protect users from bad actors accessing their accounts.

Those who remain locked out of their Apple accounts have often lost something irreplaceable.

Right after her iPhone was stolen outside the New York bar, Ms. Ayas, who holds a graduate degree in economics from Princeton University, tried to log into her Apple ID and access Find My iPhone. By that point the thief had already changed her password. Months and numerous calls to Apple support later, she still is unable to get back into her account because the thief also enabled the recovery key.

“I go to my Photos app and scroll up, hoping to see familiar faces, photos of my dad and my family—they’re all gone,” Ms. Ayas said. “Being told permanently that I’ve lost all of those memories has been very hard.”