Public Service Announcement
FEDERAL BUREAU OF INVESTIGATION

June 10, 2020

Alert Number
I-061020-PSA

Questions regarding this PSA should be directed to your local **FBI Field Office**.

Local Field Office Locations: www.fbi.gov/contact-us/field

Increased Use of Mobile Banking Apps Could Lead to Exploitation

As the public increases its use of mobile banking apps, partially due to increased time at home, the FBI anticipates cyber actors will exploit these platforms.

Americans are increasingly using their mobile devices to conduct banking activities such as cashing checks and transferring funds. US financial technology providers estimate more than 75 percent of Americans used mobile banking in some form in 2019.

Studies of US financial data indicate a 50 percent surge in mobile banking since the beginning of 2020. Additionally, studies indicate 36 percent of Americans plan to use mobile tools to conduct banking activities, and 20 percent plan to visit branch locations less often. With city, state, and local governments urging or mandating social distancing, Americans have become more willing to use mobile banking as an alternative to physically visiting branch locations. The FBI expects cyber actors to attempt to exploit new mobile banking customers using a variety of techniques, including app-based banking trojans and fake banking apps.

App-Based Banking Trojans

The FBI advises the public to be cautious when downloading apps on smartphones and tablets, as some could be concealing malicious intent. Cyber actors target banking information using banking trojans, which are malicious programs that disguise themselves as other apps, such as games or tools. When the user launches a legitimate banking app, it triggers the previously downloaded trojan that has been lying dormant on their device. The trojan creates a false version of the bank's login page and overlays it on top of the legitimate app. Once the user enters their credentials into the false login page, the trojan passes the user to the real banking app login page so they do not realize they have been compromised.

Fake Banking Apps

Actors also create fraudulent apps designed to impersonate the real apps of major financial institutions, with the intent of tricking users into entering their login credentials. These apps provide an error message after the attempted login and will use smartphone permission requests to obtain and bypass security codes texted to users. US security research organizations report that in 2018, nearly 65,000 fake apps were detected on major app stores, making this one of the fastest growing sectors of smartphone-based fraud.

TIPS TO PROTECT YOU AND YOUR ORGANIZATION

Obtain Apps from Trusted Sources

Private sector companies manage app stores for smartphones and actively vet these apps for malicious content. Additionally, most major US banks will provide a link to their mobile app on their website. The FBI recommends only obtaining smartphone apps from trusted sources like official app stores or directly from bank websites.

Use Two-Factor Authentication

Since 2016, surveys of application and website users have identified that a majority of users do not enable two-factor authentication when prompted. These users cite inconvenience as the major reason to avoid the use of this technology. Cybersecurity experts have stressed that two-factor authentication is a highly effective tool to secure accounts against compromise, and enabling any form of two-factor authentication will be to the user's advantage.

Do:

- Enable two-factor or multi-factor authentication on devices and accounts to protect them from malicious compromise.
- Use strong two-factor authentication if possible via biometrics, hardware tokens, or authentication apps.
- Use multiple types of authentication for accounts if possible. Layering different authentication standards is a stronger security option.
- Monitor where your Personal Identifiable Information (PII) is stored and only share the most necessary information with financial institutions.

Don't:

- Click links in e-mails or text messages; ensure these messages come from the financial institution by double-checking e-mail details. Many criminals use legitimate-looking messages to trick users into giving up login details.

- Give two-factor passcodes to anyone over the phone or via text. Financial institutions will not ask you for these codes over the phone.

Use Strong Passwords and Good Password Security

Cyber actors regularly exploit users who reuse passwords or use common or insecure passwords. The FBI recommends creating strong, unique passwords to mitigate these attacks. The National Institute of Standards and Technology's most recent guidance encourages users to make passwords or passphrases that are 15 characters or longer.

Do:

- Use passwords that contain upper case letters, lower case letters, and symbols.
- Use a minimum of eight characters per password.
- Create unique passwords for banking apps.
- Use a password manager or password management service.

Don't:

- Use common passwords or phrases, such as "Password1!" or "123456."
- Reuse the same passwords for multiple accounts.
- Store passwords in written form or in an insecure phone app like a notepad.
- Give your password to anyone. Financial institutions will not ask you for this information over the phone or text message.

If a Banking App Appears Suspicious, Call the Bank

If you encounter an app that appears suspicious, exercise caution and contact that financial institution. Major financial institutions may ask for a banking PIN number, but will never ask for your username and password over the phone. Check your bank's policies regarding online and app account security. If the phone call seems suspicious, hang up and call the bank back at the customer service number posted on their website.