Public Service Announcement

FEDERAL BUREAU OF INVESTIGATION

March 16, 2022

Alert Number
I-031622-PSA

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

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

Technical and Customer Support Fraud

Tech and Customer Support Fraud involves a criminal posing as technical or customer support/service to defraud unwitting individuals. Criminals may offer support to resolve such issues as a compromised email or bank account, a virus on a computer, or a software license renewal. Recent complaints involve criminals posing as customer support for financial institutions, utility companies, or cryptocurrency exchanges.

Many victims report being directed to make wire transfers to overseas accounts or purchase large amounts of prepaid cards. The use of cryptocurrency and cryptocurrency ATMs is also an emerging method of payment.

Tech support scammers continue to impersonate well-known tech companies, offering to fix non-existent technology issues, renewing fraudulent software, or security subscriptions. In 2021, the IC3 observed an increase in complaints reporting the impersonation of customer support, which has taken on a variety of forms.

- **Banking support impersonators**: Victims are usually contacted telephonically or via text to indicate a problem with the customer's account and the victim is persuaded to allow access to their computer and bank account to correct the issue. The scammer utilizes the access to initiate transfers from the account and others associated with it. By the time the victim realizes what occurred, the account is often empty.
- **Cryptocurrency support impersonators**: Cryptocurrency is still a new currency unfamiliar to most. Increasingly, crypto-owners are falling victim to scammers impersonating support or security from cryptocurrency exchanges.
    - Owners are cold-contacted via call, text, or email alerting them to a security problem with their crypto wallet and are convinced to either grant access to their crypto wallet or transfer the contents of their wallet to another wallet to "safeguard" the contents.
    - Crypto-owners are also searching online for support with their crypto wallets and transactions. Fraudsters will create fictitious support sites to entice crypto-owners to contact them directly and convince them to divulge login information or control of their crypto accounts.
- **Drivers employed by ride-share or transportation mobility companies**: Drivers report being contacted by someone impersonating support staff of their rideshare company with an issue regarding a rider complaint or the driver's account. The driver is convinced to allow access to their account and all funds in the account are taken by the impersonator.

- **Utility, cable, or internet companies**: Victims report being contacted by someone impersonating a utility company with claims of an unpaid bill they must pay immediately to avoid shutoff; or contacted by a cable, phone, or internet company with offers of great savings.
- **Travel industry:** Scammers are impersonating customer support of the car rental, airline, and hotel industries with offers of great deals or taking fake reservations. Payment is usually requested by prepaid cards. Unsuspecting victims report to a reservation counter, only to find no car, hotel, or flight reservation exists.

SUGGESTIONS FOR PROTECTION

- Legitimate customer, security, or tech support companies will not initiate unsolicited contact with individuals.
- Install ad-blocking software to reduce reduce pop-ups and malvertising (online advertising to spread malware). Ensure all computer anti-virus, security, and malware protection is up to date.
- Be cautious of customer support numbers obtained via open source searching. Phone numbers listed in a “sponsored” results section are likely boosted as a result of Search Engine Advertising.
- Resist the pressure to act quickly. Criminals will urge the victim to act fast to protect their device or account.
- Do not give unknown, unverified persons remote access to devices or accounts.

IF YOU ARE A VICTIM

- Run up-to-date virus scan software to check for potentially malicious software installed by the scammers. Consider having your computer professionally cleaned.
- Contact your financial institutions immediately. Take steps to protect your identity and your accounts.
- Change all passwords if the scammer had access to your device.
- Expect additional attempts at contact. The scammers often share their victim database information.
- File a complaint with the IC3, www.ic3.gov. If possible, include the following:
    - Identifying information of the criminal and company, including web sites, phone numbers, and e-mail addresses or any numbers you may have called.
    - Account names, phone numbers, and financial institutions receiving any funds (e.g., bank accounts, wire transfers, prepaid card payments, cryptocurrency wallets) even if the funds were not actually lost.
    - Description of interaction with the criminal.
    - The e-mail, Web site, or link that caused a pop-up or locked screen.
- Keep all original documentation, e-mails, faxes, and logs of all communications.