FBI Boston
Kristen Setera
(857) 386-2905

October 18, 2022

FBI Warns Public to Beware of Tech Support Scammers Targeting Financial Accounts Using Remote Desktop Software

The Boston Division of the Federal Bureau of Investigation (FBI) is warning that as tech support fraud evolves, the number of people falling victim to the crime is on the rise, and so are financial losses. Investigators are seeing an emerging trend in which tech support scammers are convincing victims that their financial accounts have been compromised and their funds need to be moved so the fraudsters can gain control over the victims' computers and finances.

In tech support scams, fraudsters pose as customer or tech support representatives from reputable well-known tech companies. They may call, email, or text their targets and offer to resolve such issues as a compromised email or bank account, a computer virus, or a software license renewal. Once they convince victims that their financial accounts have been compromised and their funds need to be moved, they gain control over the victims' computers and ultimately their finances.

Victims are often directed to wire or transfer their funds out of brokerage or bank accounts to cryptocurrency exchanges, or to transfer the contents of their crypto wallet to another wallet to "safeguard" the contents. Fraudsters will create fictitious support sites to entice crypto owners to contact them directly and convince them to divulge login information or surrender control of their crypto accounts.

Scammers are also asking victims to install free, remote desktop software on their computers to allow them to monitor, manipulate, and perform actions within the victims' computers such as opening virtual currency accounts to facilitate the liquidation of their genuine bank accounts.

"Cybercriminals are constantly coming up with new ways to rip off unsuspecting consumers, and this latest tactic has resulted in staggering losses. In some cases, we've seen victims lose their entire life savings which is why we are urging everyone, especially our aging family members and friends, to heed this warning," said Joseph R. Bonavolonta, special agent in charge of the FBI Boston Division. "Anyone who is a victim of this type of intrusion should report the compromise to us to help prevent these predators from victimizing others, and potentially from re-victimizing you."

Legitimate customer and tech support representatives will never initiate unsolicited contact with customers. They will not demand immediate payment or request payment via cash, prepaid gift cards, wire transfers, or cryptocurrency either.

According to the FBI's Internet Crime Compliant Center (IC3), which provides the public with a means of reporting Internet-facilitated crimes, there has been a steady increase in losses by victims in a wide-variety of tech support scams in the last five years.

Nationwide, in 2021, 23,903 people reported losing more than $347 million due to tech support scams which is a 137% increase in losses from the previous year. Most victims, almost 60%, reported to be over 60 years old, and experienced 68% of the losses. Here in the Boston Division, which includes all of Maine, Massachusetts, New Hampshire, and Rhode Island, 809 victims reported losing more than $7.5 million which is a 49% jump from the previous year. Locally, 60% of victims reported to be over 60 years old and accounted for 77% of the losses.

- 106 victims in Maine lost $673,339
- 521 victims in Massachusetts lost $5,386,594
- 117 victims in New Hampshire lost $568,394
- 65 victims in Rhode Island lost $915,714

The reported losses are most likely much higher because older Americans are less likely to report fraud due to the fact that they either don't know how to report it, are embarrassed, or don't know they have been scammed.

Several incidents recently reported include:

A couple from Maine lost $1.1 million after receiving a pop-up alert advising them their computer had been breached and there was an attempt to compromise their banking information. The couple was asked to call someone who was purportedly with Fidelity Investments and was told to download UltraViewer software on their computer so that "Microsoft" and "Fidelity" representatives could monitor for any additional fraudulent activity. The fraudsters convinced the couple to wire funds from their retirement account to Coinbase and told them to take out a home equity line of credit and wire those funds to Coinbase for "safekeeping" before the scammers eventually cut off all contact with them.

A New Hampshire resident lost approximately $1 million after receiving a pop-up alert advising she had been "hacked." After calling the tech support number, a man with a foreign accent advised her that several bank accounts had been compromised and child pornography was downloaded on her computer. The fraudster offered to "help," and asked her to download remote desktop software. Over the next six months, the victim was told to buy tens of thousands of dollars' worth of gift cards, scratch off the numbers, and relay that information to him so he could convert the money to bitcoin to protect her accounts. She was then asked to wire the remaining assets in her retirement account to her bank account so she could withdraw the cash and deposit it into various bitcoin machines.

A Rhode Island woman lost $200,000 after browsing online and receiving a pop-up alert that stated her iPad was compromised and she needed to call Apple support. She was instructed to download "AnyDesk," a remote desktop application, and was then told her ID was used to purchase child pornography. The tech support rep transferred her to someone who was purportedly with Fidelity Investments to help her address the fraudulent charges. The person at "Fidelity" advised that child pornography was illegal, she should not disclose that it was found on her computer to anyone, and if she did not address it, it would be tied to her social security account. She was told by "Fidelity" they were going to cancel the charges and send her money to a dummy account to prevent additional fraud. She was told to make three separate wire transfers and the money would return to her within 48 hours.

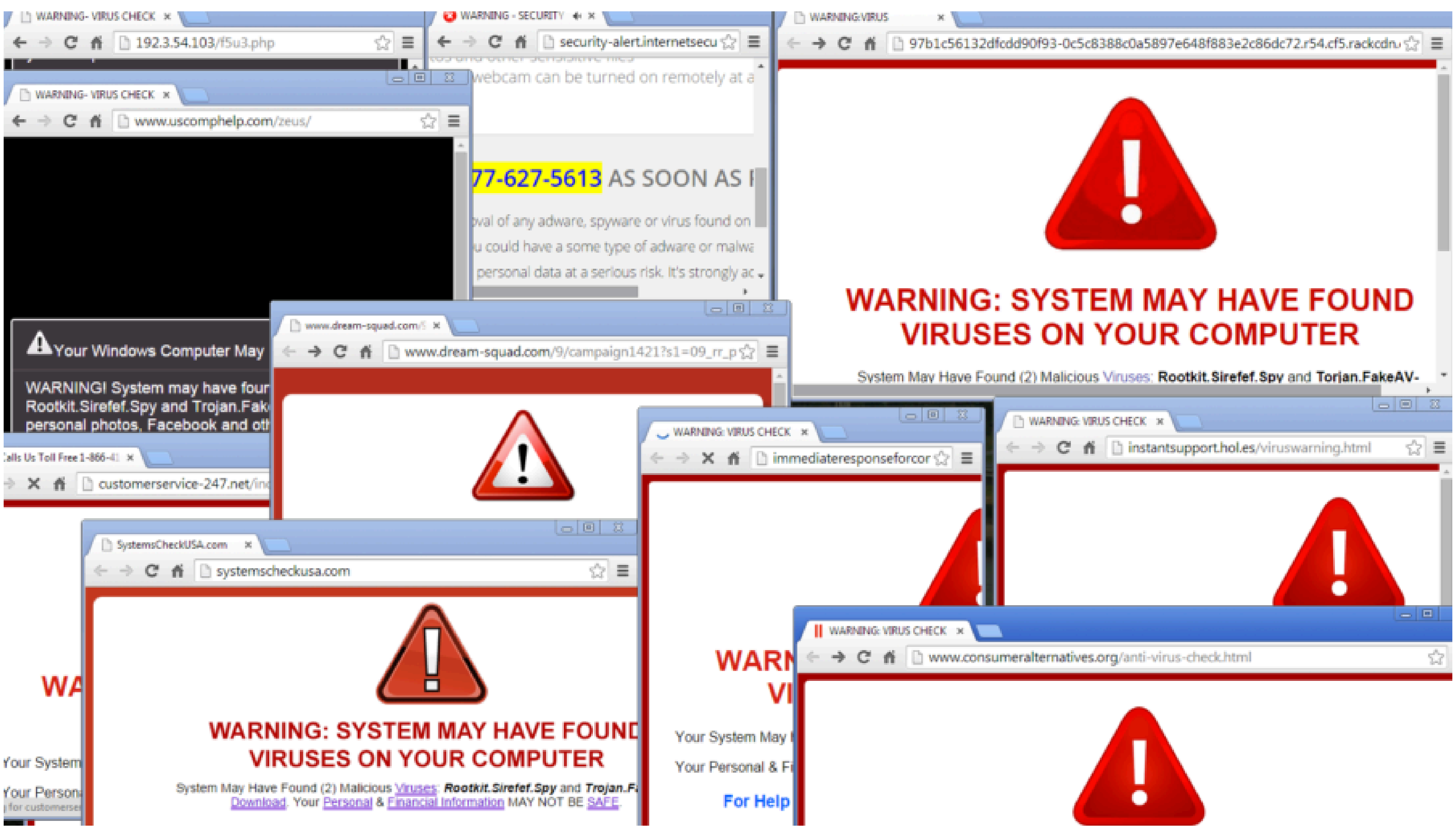
A Massachusetts woman lost approximately $200,000 after receiving a pop-up alert advising her that her computer had been "hacked." After calling the number she was given, she was routed to the "fraud" department and was told money was taken from her bank account and it was enroute to a gambling facility in Europe. The "fraud" department asked her to contact her bank to transfer her money into "safe wallets" so the hackers could not access the remainder of her funds. Over the next few weeks, the "fraud" department representative via telephone calls and messages had her wire the money held in her bank, credit union, and retirement accounts, into accounts at other banks in other people's names. The victim was advised to tell her bank that she knew the people she was transferring the money to, and the "fraud" department representative told her not to tell anyone about him because the hackers and scammers were all around her.

Suggestions for Protection:

- Legitimate customer, security, or tech support companies will not initiate unsolicited contact with individuals.
- Ensure computer anti-virus, security and malware protection is up to date and settings are enabled to reduce pop-ups.
- Be cautious of customer support numbers obtained via online searching. Phone numbers listed in a "sponsored" results section are likely boosted as a search of Search Engine Advertising.
- If a pop-up or error message appears with a phone number, don't call the number. Error and warning messages never include phone numbers.
- 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.
- Do not download or visit a website that an unknown person may direct you to.
- Do not trust caller ID readings as criminals often spoof names and numbers to appear legitimate. Let unknown numbers go to voice mail and do not call unknown numbers back.
- Never trust any company-tech or otherwise-requesting personal or financial information.

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 by using the number on the back of your bank card or by visiting the institution in person. 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.
- Keep all original documentation, emails, faxes, and logs of all communications.
- File a police report at your local police station.
- File a complaint with the FBI's Internet Crime Complaint Center at www.ic3.gov. If possible, include the following:
  - Identifying information of the criminal and company, including websites, phone numbers, and email 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 email, website, or link that caused a pop-up or locked screen.


WARNING- VIRUS CHECK
192.3.54.103/f5u3.php
WARNING - SECURITY
security-alert.internetsecu
WARNING:VIRUS
97b1c56132dfcdd90f93-0c5c8388c0a5897e648f883e2c86dc72.r54.cf5.rackcdn
www.uscomphelp.com/zeus/
webcam can be turned on remotely at a
77-627-5613 AS SOON AS I
WARNING: SYSTEM MAY HAVE FOUND VIRUSES ON YOUR COMPUTER
System May Have Found (2) Malicious Viruses: Rootkit.Sirefef.Spy and Trojan.FakeAV-
Your Windows Computer May
WARNING! System may have found Rootkit.Sirefef.Spy and Trojan.Fak personal photos, Facebook and oth
www.dream-squad.com/9/campaign1421?s1=09_n_p
customerservice-247.net
immediateresponseforcor
instantsupport.hol.es/viruswarning.html
systemscheckusa.com
WARNING: SYSTEM MAY HAVE FOUND VIRUSES ON YOUR COMPUTER
System May Have Found (2) Malicious Viruses: Rootkit.Sirefef.Spy and Trojan.F Download. Your Personal & Financial Information MAY NOT BE SAFE.
Your System May
Your Personal & Fi
For Help
www.consumeralternatives.org/anti-virus-check.html

Most Wanted
Ten Most Wanted
Fugitives
Terrorism
Kidnappings / Missing Persons
Seeking Information
Bank Robbers
ECAP
ViCAP

FBI Jobs
Submit a Tip
Crime Statistics
History
FOIPA
Scams & Safety
FBI Kids

News
Stories
Videos
Press Releases
Speeches
Testimony
Podcasts and Radio
Photos
Español
Apps

How We Can Help You
Law Enforcement
Victims
Parents and Caregivers
Students
Businesses
Safety Resources
Need an FBI Service or More Information?

What We Investigate
Terrorism
Counterintelligence
Cyber Crime
Public Corruption
Civil Rights
Organized Crime
White-Collar Crime
Violent Crime
WMD

About
Mission & Priorities
Leadership & Structure
Partnerships
Community Outreach
FAQs

Contact Us
Field Offices
FBI Headquarters
Visit the FBI Experience
Overseas Offices

Additional Resources
Accessibility
eRulemaking
Freedom of Information / Privacy Act
Legal Notices
Legal Policies & Disclaimers
Privacy Policy
USA.gov
White House
No FEAR Act
Equal Opportunity

FBI FEDERAL BUREAU OF INVESTIGATION

FBI.gov Contact Center