

# Welcome



TEXAS ★ BANKING ★ ORIGINAL



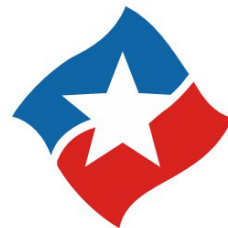
# Annual Cybersecurity Event



**Practical Tips for Cybersecurity:**

# **Protecting Your Business**

# **Protecting The Community**



TexasBankers  
Association  
*Strong Banks. Stronger Communities.*



**Your customers are your business**  
**Your network is your business**



# Background

- White House Office of Homeland Security
- US Department of Homeland Security
- Ridge Global
- US Chamber of Commerce Cyber Leadership Council
- State of Texas Cybersecurity Council



JOINT STATEMENT BY THE FEDERAL BUREAU OF INVESTIGATION (FBI), THE CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY (CISA), THE OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE (ODNI), AND THE NATIONAL SECURITY AGENCY (NSA)

Original release date: January 16, 2021



On behalf of President Trump, the National Security Council staff has stood up a task force construct known as the Cyber Unified Coordination Group (CUCG), composed of the FBI, CISA, and ODNI with support from NSA, to coordinate the investigation and remediation of this significant cyber incident involving federal government networks. The CUCG is still working to understand the scope of the incident but has the following updates on its investigative and mitigation efforts.

This work indicates that an Advanced Persistent Threat (APT) actor, likely Russian in origin, is responsible for most or all of the recently discovered, ongoing cyber compromises of both government and non-governmental networks. At this time, we believe this was, and continues to be, an intelligence gathering effort. We are taking all necessary steps to understand the full scope of this campaign and respond accordingly.

The CUCG believes that, of the approximately 14,000 affected public and private sector customers of Solar Winds' Orion product, a much smaller number have been compromised by follow on activity on their systems. We have so far identified fewer than ten U.S. government agencies that fall into this category, and are working to identify and notify the management entities who also may be impacted.

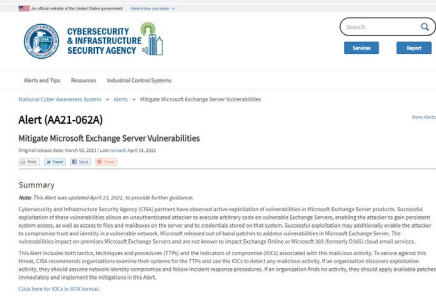
This is a serious compromise that will require a sustained and dedicated effort to remediate. Since its initial discovery, the CUCG, including hardworking professionals across the United States Government, as well as our private sector partners have been working non-stop. These efforts did not let up through the holidays. The CUCG will continue taking every necessary action to investigate, remediate, and share information with our partners and the American people.

As the lead agency for threat response, the FBI's investigation is presently focused on four critical lines of effort: identifying victims, collecting evidence, analyzing the evidence to determine further attribution, and sharing results with our government and private sector partners to inform operations, the intelligence picture, and network defenses.

As the lead for asset response, CISA is focused on sharing information quickly with our government and private sector partners as we work to understand the extent of this campaign and the level of exploitation. CISA has also created a free tool for detecting unusual and potentially malicious activity related to this incident. In an Emergency Directive posted December 14, CISA directed the rapid disclosure or power-down of affected SolarWinds Orion products from federal networks. CISA also issued a technical alert providing technical details and mitigation strategies to help network defenders take immediate action. CISA will continue to share any known details as they become available.

As the lead for intelligence support and related activities, ODNI is coordinating the intelligence Community to ensure the ICSS has the most up-to-date intelligence to drive United States Government mitigation and response activities. Further, as part of its information-sharing mission, ODNI is providing situational awareness for key stakeholders and coordinating intelligence collection activities to address knowledge gaps.

Lastly, the NSA is supporting the CUCG by providing intelligence, cybersecurity expertise, and actionable guidance to the CUCG partners, as well as National Security Systems, Department of Defense, and Defense Industrial Base system owners. NSA's engagement with both the ICSS and industry partners is focused on assessing



# Sophisticated Actors:

- China
- Russia
- Iran
- Global Criminal Organizations



## Russia blamed for SolarWinds hack in joint FBI, NSA and CISA statement

The US intelligence agencies investigating the widespread compromise say it was "likely" orchestrated from Russia



The SolarWinds attack likely came from Russia, the FBI has said.  
CHET/Aminda Kooser

Key government intelligence agencies said Tuesday that the SolarWinds hack is "likely Russian in origin," according to a joint statement from the FBI, NSA, Cybersecurity and Infrastructure Security Agency and Office of the Director of National Intelligence. It's the first time the four agencies have attributed the cyber attack to Russia.

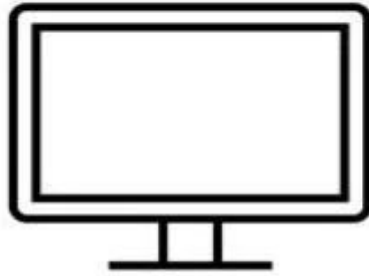
"This work indicates that an Advanced Persistent Threat (APT) actor, likely Russian in origin, is responsible for most or all of the recently discovered, ongoing cyber compromises of both government and non-governmental networks," the statement said. "At this time, we believe this was, and continues to be, an intelligence gathering effort."



# FBI: COMMON THREATS TO BUSINESS

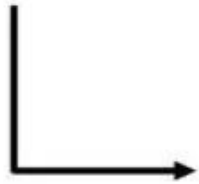
- [Data breaches](#) can reveal trade secrets, proprietary material, and customer data.
- [Business email compromise \(BEC\)](#) scams exploit the fact that so many of us rely on email to conduct business—both personal and professional—and it's one of the most financially damaging online crimes. Messages often convey a sense of urgency.
- [Ransomware](#) is a type of malicious software, or malware, that prevents you from accessing your computer files, systems, or networks and demands you pay a ransom for their return.
- [Spoofing and phishing](#) are schemes aimed at tricking you into providing sensitive information to scammers.

# Phantom Hacker Scam



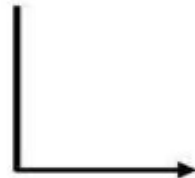
## Tech Support Imposter

- Pretends to be technical support
- Will want to install software on your computer, look at finances



## Financial Institution Imposter

- Says computer & finances have been accessed by hackers
- tells you to move money to a 3<sup>rd</sup> party account for "safety"



## US Government Imposter

- Will identify themselves as US government employee
- May provide official looking letterhead as proof of legitimacy



“From January through June of this year, there were **19,000 tech support scams** reported to the FBI Internet Crime Complaint Center; more than **\$542 million was lost** during that time frame. The losses this year already exceed 2022 losses by **40 percent.**”

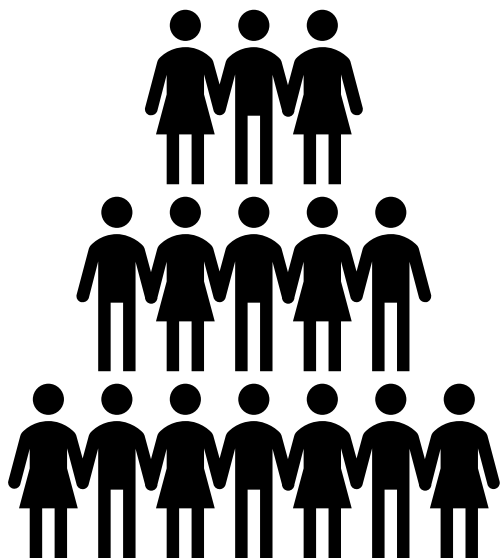


*What can I do?*

## FBI GENERAL RECOMMENDATIONS

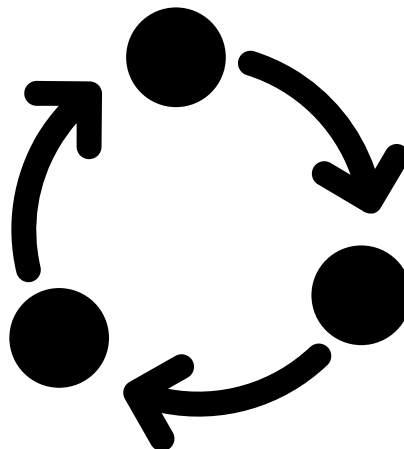
- Keep systems and software up to date and install a strong, reputable anti-virus program.
- Be careful when connecting to a public Wi-Fi network and do not conduct any sensitive transactions, including purchases, when on a public network.
- Create a strong and unique passwords for each online account and change them regularly.
- Set up multi-factor authentication (MFA) on all accounts that allow it.

P



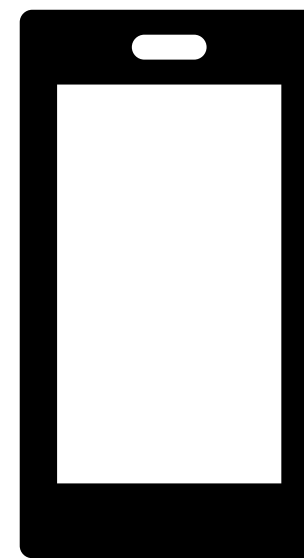
People

P



Processes

T



Technology

# CYBERSECURITY RISK IS A PEOPLE PROBLEM AS MUCH AS IT IS A TECHNOLOGY PROBLEM



“Gone Phishing”: Social engineering schemes, the go-to for nefarious cyber actors, remain effective.

“Insiders were the source for 50% of incidents where private or sensitive information was unintentionally exposed.”\*





*What can I do?*

# RECOMMENDATIONS FOR YOUR BUSINESS

## Consider your external relationships

- Get recommendations for reputable service providers
- Interview vendors and third-party providers
- Maintain a relationship w/ regular “check-ins”
- Incident response: Know what you can expect if there is a problem and get it in writing whenever possible



*What can I do?*

## RECOMMENDATIONS FOR YOUR BUSINESS

### Have internal policies & controls

- Know who has access
- Establish policies about who can use systems and when
- Establish rules for appropriate usage of systems
- Train employees on security and policies
- Immediately “Off-Board” former employees/users/third-parties



***What can I do?***

# **RECOMMENDATIONS FOR YOUR BUSINESS**

## **Have internal policies & controls**

- Have policies for validating major financial transactions
- Major transactions should not be authorized by email or text messages without discussion (call back policy)
- Policy wrap-up:
  - If you don't have written policies, you don't have policies
  - If policies are not effectively communicated, you don't have policies



## Data Breach Reporting

Texas law requires businesses and organizations that experience a data breach of system security that affects 250 or more Texans to report that breach to the Office of the Texas Attorney General as soon as practicably possible and no later than 30 days after the discovery of the breach. Businesses and organizations must also provide notice of the breach to affected consumers.

Effective September 1, 2023, Texas law requires that all reports be submitted to the Texas Attorney General electronically using the Data Breach Report provided by the OAG. The report to the AG must specify the number of Texans that the business or organization has notified of the breach by mail or email.

If you are an *individual* that has been notified of a data breach, and/or are not an authorized representative of the business or organization experiencing a data breach, please [submit your information via a consumer complaint form](#).

<https://www.texasattorneygeneral.gov/consumer-protection/data-breach-reporting>

**Acts 2023, 88th Leg., R.S., Ch. 246 (S.B. 768), Sec. 1**  
**Effective September 1, 2023.**



# Don't Just Buy Insurance— Get Assurance

---

Who procures your cyber insurance?

Does the procurement officer coordinate with your IT team?

Does your insurance reflect what you know from assessments?

Or did you just buy a policy?

Do you know what your cyber insurance will cover? Not cover?

**Social Media Transfer Exclusion** - The **Insurer** will not be liable to make any payment for **Loss, Regulatory Correction Expense, Public Relations Expense, or Privacy Breach Response Expense** in connection with any **Claim, Privacy Breach Incident, or Denial of Service Attack** arising out of, or in any way involving the transfer of funds or currency through social media, including the **Company's** own **Social Networking** profiles and accounts.

**Subsidiary Wrongful Acts Exclusion** - The **Insurer** will not be liable to make any payment for **Loss or Regulatory Correction Expense** in connection with any **Claim** involving any **Subsidiary** or its **Insured Persons** acting in the capacity of director, member of the board of trustees, officer or **Employee** of such **Subsidiary** for any **Wrongful Internet/Electronic Banking Act or Interrelated Wrongful Internet/Electronic Banking Acts** actually or allegedly committed in whole or in part at any time when the entity was not a **Subsidiary** except as provided in Section XI (C)(3). The **Insurer** will also not be liable to make any payment for **Loss, Regulatory Correction Expense, Public Relations Expense or Privacy Breach Response Expense** in connection with any **Privacy Breach Incident or Denial of Service Attack** that began or occurred at any time when the entity was not a **Subsidiary** except as provided in Section XI (C)(3).

**Trade Secrets Exclusion** - The **Insurer** will not be liable to make any payment for **Loss, Regulatory Correction Expense, Public Relations Expense, or Privacy Breach Response Expense** in connection with any **Claim, Privacy Breach Incident, or Denial of Service Attack** arising out of or in any way involving actual or alleged misappropriation of trade secrets or proprietary information.

**Trust Services Exclusion** - The **Insurer** will not be liable to make any payment for **Loss, Regulatory Correction Expense, Public Relations Expense, or Privacy Breach Response Expense** in connection with any **Claim, Privacy Breach Incident, or Denial of Service Attack** arising out of or in any way involving the rendering or failing to render **Trust Services**. But this exclusion does not apply to:

- (1) **Claims** alleging invasion of privacy; libel; slander; defamation; other actionable oral or written disparagement; loss or damage to **Electronic Data** of a **Customer**; unauthorized access to a **Customer** account maintained by the **Company**; infringement of copyright; misappropriation of ideas (other than patent infringement); plagiarism; or infringement of trademark, trade name or service mark; or
- (2) **Loss** covered under any Business Interruption or Cyber/Network Extortion Insuring Agreement attached to this **Policy** (if applicable).

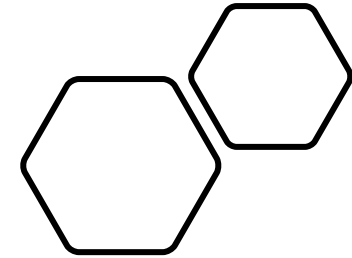
**Utility Service/Internet Failure Exclusion** - The **Insurer** will not be liable to make any payment for **Loss, Regulatory Correction Expense, Public Relations Expense, or Privacy Breach Response Expense** in connection with any **Claim, Privacy Breach Incident, or Denial of Service Attack** arising out of or in any way involving the interruption or failure of the Internet, any power or other utility service, any satellite, or any component part or infrastructure support thereof.

**War Exclusion** - The **Insurer** will not be liable to make any payment for **Loss, Regulatory Correction Expense, Public Relations Expense, or Privacy Breach Response Expense** in connection with any **Claim, Privacy Breach Incident, or Denial of Service Attack** arising out of, or in any way involving or attributable to, acts of war, acts of foreign enemies, the acts of any military organization, or the acts of any government regardless of any other contributing cause or event.

#### SECTION VI - LIMIT OF LIABILITY AND RETENTION

##### A. **LIMIT OF LIABILITY**

- 1) Subject to paragraph A.2, below, if a **Claim, Privacy Breach Incident or Denial of Service Attack** is covered by more than one Insuring Agreement, the **Insurer's** maximum Limit of Liability for such **Claim, Privacy Breach Incident or Denial of Service Attack** shall not exceed the highest Limit of Liability provided by any Insuring Agreement providing coverage to the **Insured**.



Do you  
understand your  
cyber policy  
**EXCLUSIONS?**






**Your bank.  
Your partner for security.**


**Monitor Your Accounts Closely  
Call your NDBT relationship banker with any concerns**

# #BanksNeverAskThat

 **Texas Bankers Association** · 2d ...


The “Pay Yourself” scam is on the rise. Don’t fall for bogus bank fraud alerts, 'cause [#BanksNeverAskThat](#). See if you can outsmart scammers with this phishing quiz from the American Bankers Association: [bit.ly/3RCoNvv](https://bit.ly/3RCoNvv)

[#StrongBanks](#)  
[#StrongerCommunities](#)

 **How the “Pay Yourself” Scam Works** ⚠️


**Step 1: You reply to a fake fraud alert text about Zelle.**  
It looks like it's from your bank, but it's a scammer impersonating your bank.

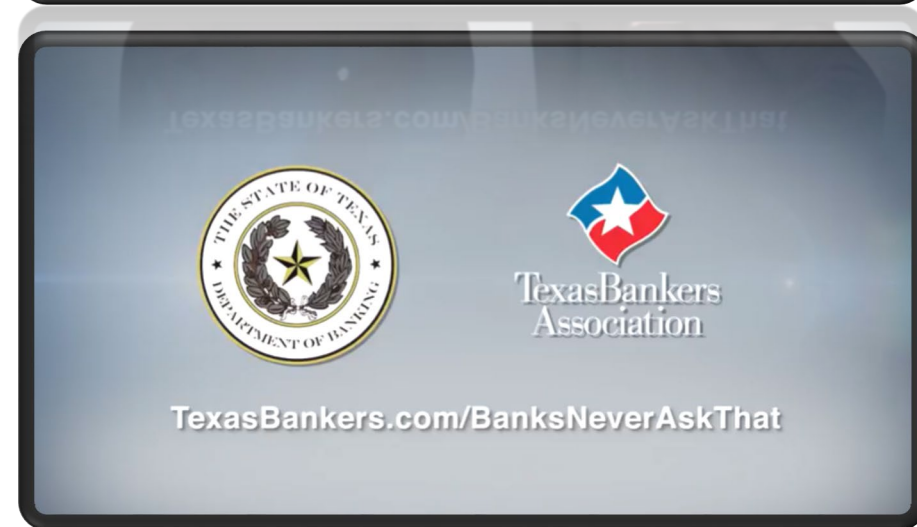
**Step 2: The scammer calls you.**  
Pretending to be the fraud department, they'll ask you to sign into Zelle and tell them the one-time passcode your bank texts you.



**Step 3: They ask you to send money to yourself.**  
Using your passcode, they've added their bank account to your Zelle to receive your money.

**Step 4: Bye-bye money.**  
Once you click send, the money is transferred to their account and the scam is complete.







# Thank you!



**TexasBankersAssociation**  
*Strong Banks. Stronger Communities.*

**NNDDBT**  
TEXAS ★ BANKING ★ ORIGINAL