INSIDER THREATS: THE RISK WITHIN

Understanding the impact, protecting your credentials, and recognizing warning signs



Kayvan Yazdi,
CEO of
TruAdvantage

OUR MISSION

Impacting our clients' success through trusting and meaningful partnerships and delivering strategic, secure, white-glove IT.

2026- CALIFORNIA WINNER
MSP 501
Channel Futures.

HIPAA COMPLIANT

SOC 2 TYPE 2

#1 RATED IT MSP ON CHATGPT
TruAdvantage

300+ Google Reviews



THIS MONTH'S TOPICS:

The Cost of Insider Threats

How They Affect Operations, Trust, and More

Your Login, Your Responsibility

Prevent Accidental Harm and Delibrate Misuse

Recognize the Risk

Spotting Unsafe Actions and Reporting Concerns

Scam of the Month:

Fake Payroll Portal Scams

Cybersecurity risks can come from people who already have access to an organization's information and systems. Whether caused by an honest mistake, an unsafe shortcut, or deliberate misuse, insider threats can expose sensitive information and damage trust. This month's newsletter explores how those consequences extend beyond the immediate financial cost.

We'll also explain why keeping your credentials private helps reduce insider risks and highlight actions that deserve attention. By protecting your access, following approved procedures, and reporting concerns promptly, you can help safeguard your organization.

The Cost of Insider Threats

A sensitive file sent to the wrong person. A coworker using someone else's login. An employee deliberately taking confidential information. These situations have different intentions, but each can put an organization at risk.

Where the Costs Add Up

Response & Recovery

Investigating an incident takes time and resources. Organizations may need to identify what happened, secure accounts, restore information, and bring in outside specialists.



Interrupted Operations



Deleted files, unauthorized changes, or compromised systems can disrupt everyday work. Employees may lose access to essential tools, projects may stall, and customers may experience delays.

Exposed Information

Customer records, employee information, financial details, and confidential business plans can be compromised. Once information has been copied or disclosed, recovering a file does not undo the exposure.



Damaged Trust



Customers and business partners expect organizations to protect their information. An incident can weaken that confidence and affect relationships long after the immediate problem is resolved.

Additional Obligations

Depending on the incident and applicable requirements, organizations may face notification expenses, legal claims, or regulatory consequences.



Your Login, Your Responsibility

“Can I use your login for a minute?”

It may sound like a small favor, especially when a coworker is facing a deadline. But sharing your credentials can give someone access to information or actions they have not been approved to use.

Credentials include passwords, PINs, and other information or tools used to access an account. Protecting them matters even when the person asking is someone you know.

How Sharing Creates Unintentional Risk

Imagine lending your account to a coworker who cannot access a system. While completing their task, they accidentally change a record or open information outside their role.

Neither person intended to cause harm. But sharing the account bypassed the organization’s access controls and created an opportunity for a mistake.

How Sharing Enables Intentional Misuse

Someone seeking to steal information or make unauthorized changes could ask to borrow another person’s account. That account might provide access their own account does not.

Activity may initially appear under the account owner’s name, making it harder to determine who actually performed an action. Trusting a coworker does not replace the need for individual, authorized access.

Help Without Handing Over Access

1. Keep your individual password and PIN private.
2. Protect your sign-in factors.
3. Use approved delegation and sharing features.
4. Lock your screen when you step away.
5. Direct access problems to IT or the approved support team.



Recognize the Risk

Insider threats do not have one recognizable personality or appearance. The most useful warning signs involve how someone handles information, uses access, or follows security procedures.

Understanding the difference between unintentional risk and possible deliberate misuse can help you recognize concerns. You do not need to determine someone's motives before reporting an unsafe action.

UNINTENTIONAL INSIDER THREATS: HARM WITHOUT MALICIOUS INTENT

These situations may involve an honest mistake, a misunderstanding, or a shortcut taken without intending to cause harm. Someone may knowingly skip a security step while failing to recognize the consequences.

Examples

1. Sending sensitive information to the wrong recipient.
2. Giving a file broader sharing permissions than intended.
3. Leaving a device unlocked or confidential paperwork exposed.
4. Using an unapproved personal account or application to complete work.
5. Sharing credentials to help a coworker finish a task.



INTENTIONAL INSIDER THREATS: POSSIBLE SIGNS OF DELIBERATE MISUSE

Intentional insider threats occur when someone deliberately uses their access to steal information, disrupt operations, or otherwise cause harm. Their actions may be motivated by financial gain, revenge, or pressure from someone outside the organization.

Examples

1. Attempting to access sensitive information unrelated to assigned work.
2. Copying or transferring confidential files to an unauthorized destination.
3. Asking to use another employee's account to bypass an access restriction.
4. Disabling security protections or attempting to erase activity records without authorization.
5. Deliberately altering, deleting, or disclosing information without permission.



SCAM OF THE MONTH: FAKE PAYROLL PORTAL SCAMS

Each month we highlight a scam that demonstrates tactics criminals are using RIGHT NOW, to better prepare you when the next scam hits.

Alex wants to check his latest paystub before paying a few bills. Instead of using the link on his company's employee resource page, he searches online for the payroll provider. A sponsored result appears near the top, and the name looks right. He clicks it and lands on a page with the familiar logo, colors, and login form. Nothing seems out of place, so he enters his username and password. When the page displays an error, Alex assumes the service is temporarily unavailable and decides to try again later.

What Alex doesn't realize is that the website was a convincing copy created by criminals. The error message helped hide the fact that the page had captured his credentials. The attackers can now attempt to use them on the real payroll portal. If they gain access, they could change his direct deposit information and send a future paycheck to an account they control. Using his company's approved link or a verified bookmark would have helped Alex avoid the fake page, and reporting the suspicious login promptly could give IT and payroll a chance to act before money goes missing.



DID YOU SPOT THE RED FLAGS?

- An advertisement led to the login page.
- The address did not match the official portal.

HOW TO PROTECT YOURSELF

- Use your organization's approved link or a verified bookmark. Access payroll and benefits portals through a trusted route instead of a search advertisement.
- Report suspected exposure immediately. If you entered credentials on a suspicious page, contact your approved IT support team.