Rocket® software

Spotting the Fake IT Worker

5 Red Flags You Can't Ignore

Mainframes handle 90% of global credit card transactions, making them irresistible targets for modern cybercriminals. But some of the biggest threats are already on the inside. Insider breaches cost US$4.99 million on average. Can you spot the risks hiding in plain sight?

5 ways to spot a fake IT worker

01 Credentials that don't add up

Weak passwords, shared logins, and outdated security measures make it easy for fake employees to sneak in. Multi-factor authentication (MFA) is a must-have.

PRO TIP

Keep an eye on login patterns—unexpected locations or odd hours are big red flags.

02 Suspicious payroll activity

Fake workers can hide on your payroll, funneling money into fraudulent accounts. Look for ghost employees or strange changes in HR records.

NOTABLE CASE

A fake payroll site in Massachusetts recently tricked state employees into giving up personal data.[1]

03 AI-enabled scams

AI tools create phishing emails and fake profiles that are nearly impossible to detect. Although they may seem trustworthy, they're designed to trick people into revealing sensitive information.

WATCH FOR

Pretexting scams, where attackers create convincing scenarios to trick employees into disclosing personal data.

04 Insider threats

Disgruntled employees or contractors can compromise your data. Some attacks are intentional, others accidental—but both are costly.

NOTABLE CASE

Scammers placed 300 fake IT workers in U.S. companies, accessing critical data to benefit North Korea.[2]

05 Compliance gaps

New regulations like GDPR and DORA demand airtight data protection. Miss one, and you'll face fines—not to mention reputational damage.

QUICK WIN

Integrate your green screen login authentication into your current Identity and Access Management (IAM) system.

1. "State employees fooled by fake payroll website farming their data" Boston.com, October 10, 2024.
2. "Charges and Seizures Brought in Fraud Scheme, Aimed at Denying Revenue for Workers Associated with North Korea" Justice.gov, May 16, 2024.

How to protect your mainframe

Secure your green screen access

Mainframe logins through terminal emulators should be protected just like any modern system. Use TLS 1.3 encryption and require MFA for all login attempts.

Leverage IAM

Control access using a centralized IAM system. This ensures that only authorized users can reach your organization's sensitive systems.

Monitor everything

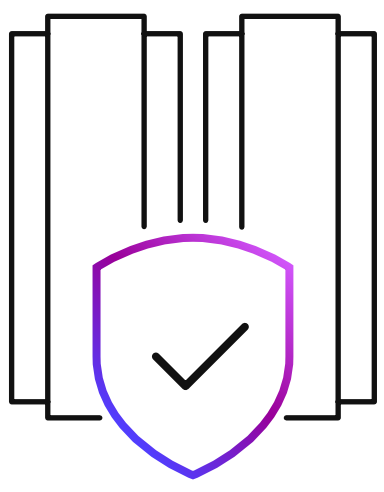
Track logins, system activity, and app usage. Real-time monitoring helps spot suspicious behavior early and prevent breaches.

Audit activity

Keep a detailed log of system interactions. This helps identify vulnerabilities and provides evidence in case of a breach.

Partner with experts

Work with security-focused vendors who stay ahead of threats and ensure compliance with regulations like GDPR and DORA.



Rocket® Secure Host Access: Your defense against fake IT workers

Provide secure, phishing-resistant, password-less access to critical host applications. With little effort, you can leverage your existing enterprise IAM and integrate host application access into your larger IT security strategy.

Secure Host Access lets you:

- Extend security best practices like SSO, SSH, and MFA.
- Redact sensitive data based on the end user's role in the organization.
- Mitigate the threat of cyberattacks and auditory fines.

Don't wait for a breach

The longer you delay securing your systems, the more vulnerable you become. Start protecting your mainframe today with Rocket Software.

Speak to an expert

Rocket® software

MAR-12282_SecureHostAccess_Infographic_V1-2