



## Workers' Comp Return-to-Work Program Best Practices

An essential component of workers' compensation is an effective return-to-work (RTW) program. Eliminating injuries and illnesses is paramount for reducing workers' compensation costs, but after an incident has occurred, an RTW program can significantly reduce workers' compensation expenses for employers and improve the lives of employees. Read on for more information on RTW programs and best practices for establishing and maintaining them.

### RTW Programs

An RTW program is characterized by specific, documented organizational policies and procedures that provide guidance to supervisors and employees in managing the RTW process following a work-related absence due to injury, illness or chronic disease. Its main goal is to expedite the individual's recovery and reintegrate them into productivity, achieved through various means such as referral, counseling, coordination of medical care, or adjustments to the workplace or job responsibilities. RTW programs may also include vocational rehabilitation services alongside transitional work options to facilitate a smooth return to full productivity.

### RTW Program Best Practices

An RTW program can assist employees in returning to work faster after a work-related illness or injury, increasing their odds of a full recovery. It also allows employers to save on workers' compensation costs. Below are best practices for employers to consider to help ensure their RTW program is effective:

- **Address the basics** by reviewing state-specific laws, outlining the roles and responsibilities of those involved in the RTW program, and setting clear expectations.
- **Put the program in writing and inform employees** about RTW policies and procedures as well as processes for filing a workers' compensation claim.

- **Establish an RTW contact person** whom an injured employee can reach out to with any questions.
- **Create a safety committee** including both management and employees. The committee can identify hazards causing injuries and illnesses and find solutions. Employee members can provide insight into the physical demands of their roles.
- **Develop functional job descriptions** that explain the physical demands and movements necessary for specific job tasks to help employers safely place employees who are returning to work after a work-related illness or injury.
- **Evaluate a returning employee's condition and modify job tasks** while they are healing. If they are unable to return to work in their previous capacity, match the employee's skills to where they can work within the company.
- **Develop individual plans** that outline necessary actions for a worker to resume their pre-illness or pre-injury role. In larger organizations, plans should be made collaboratively by the RTW program coordinator, the injured worker, the worker's supervisor, the health care provider, the union representative and legal counsel, if applicable.
- **Maintain a job duty bank** that lists jobs coordinated with doctor restrictions that employees can be placed into when they have restrictions from a work-related illness or injury.
- **Communicate** early and often with impacted workers.
- **Integrate and coordinate with all stakeholders** to share information while maintaining a focus on employees' well-being of employees.
- **Monitor, evaluate and adjust the program** by looking at the measurements they should have in place, setting up ways to gather the important data needed to review the RTW program, and continuing to adjust where necessary.

RTW programs that follow best practices provide benefits to employers and employees as they work toward full-time, full-duty work. For more RTW guidance, contact us today.

## Mitigating the Risk of Formjacking

As businesses increasingly rely on online transactions, cybercriminals have developed a scheme known as formjacking to steal sensitive data. Formjacking poses significant risks to businesses, as it is difficult to stop and can lead to major financial losses and reputational damage. This article provides more information on formjacking and offers tips on how to prevent it.

### What Is Formjacking?

Formjacking is a cyberattack in which a threat actor injects malicious JavaScript into a website, often one that contains an online payment form. Once the targeted page has been compromised, the added code permits the hacker to collect sensitive data, such as credit card numbers, addresses and phone numbers. This data is sent to the cyberattacker's domain after unsuspecting users enter their information and click "submit" to complete a transaction. Malicious actors can then use the stolen data in identity theft schemes, payment card fraud scams and account takeover attacks, or they can sell it to other criminals. Stolen information can also be used to create fraudulent accounts to distribute malware.

Formjacking attacks can have significant financial consequences, including costly lawsuits, fines, fees and penalties, as well as expenses related to remediation. Moreover, formjacking attacks can damage a company's reputation.

### Preventing Formjacking

Formjacking is challenging to detect because the malicious code frequently changes, making it difficult for external scanners and firewalls to catch it. Additionally, there are no apparent signs of formjacking, and the intended transaction is not affected, making it hard to identify and stop the scam. However, there are still several measures businesses can take to identify potential issues and reduce the risk of formjacking from occurring. Consider the following strategies:

- **Practice good cyber hygiene** by keeping software, patches and extensions up to date. Establishing a content security policy and using firewalls and subresource integrity tags can also help prevent the injection of malicious data onto business websites and protect data. Additionally, complying with security standards and educating IT staff on the threats of formjacking are essential.
- **Utilize cyberdefense techniques**, such as obfuscating JavaScript, which can make code harder for cyberattackers to understand. Additionally, implementing network segmentation can limit network exposures and malicious actors' lateral movement capabilities. An intrusion detection and prevention system can also help monitor potential threats and identify cyber intruders.
- **Implement ongoing cybersecurity measures**, such as thoroughly testing websites before they are publicly launched, executing penetration testing to discover weaknesses, and monitoring the supply chain to ensure vendors whose code is being used follow cybersecurity best practices.
- **Scan and audit website code regularly** to check its integrity. Monitoring and analyzing web logs and JavaScript behavior can help detect malicious activity, and examining where a browser is sending data is key in stopping formjacking attacks.

Layering defenses can reduce a business's vulnerability. In addition, companies should consider utilizing artificial intelligence to help detect suspicious behavior.

Formjacking is a cyberthreat that can significantly impact a business's finances, operations and reputation. Because of this, companies should take steps to prevent it. Contact us today for more information.



A cybercriminal's malicious code in a **formjacking attack** may be loaded through various methods, such as by exploiting a vulnerability in a business's website, employing a phishing scam in which the hacker gains access to a company's checkout page, or compromising a third party's app or JavaScript used by a business.

