SAFETY TIP OF THE WEEK

FOR THE CONSTRUCTION INDUSTRY

Company _____ **Date** _____

To encourage all of us to promote safety on a continuing basis, the Builders Exchange publishes a safety tip in each issue of the weekly Bulletin. The superintendent/foreman of each job should use this safety tip in a short safety meeting Monday morning. We suggest that this 5-to-10 minute meeting be just before lunch or perhaps right after the morning break. You can then emphasize the SAFETY TIP OF THE WEEK all week long.

Cybersecurity Awareness Month

Week Ending 10/20/2023

October is National Cybersecurity Awareness Month, and 2023 marks the 20th anniversary of the commemorative event. This year's theme is "Secure Our World," a public service campaign created by the Cybersecurity and Infrastructure Security Agency (CISA) at the behest of the United States Congress.

With digital threats on the rise and IT complexity increasing, it's more than just a slogan—"Secure Our World" is all about encouraging individuals and businesses to adopt better cybersecurity habits and improve online behavior.

This represents the perfect opportunity to assess the state of your company's protection. For most businesses, that starts with a realistic assessment of today's biggest risks: ransomware, phishing attacks, and data breaches. These tactics are increasingly common and can negatively impact any organization—big or small, in any industry, located anywhere in North America. So it's imperative to address them first.

But comprehensive cybersecurity protection extends much further, encompassing data backup, identity management, login protections, and real-world training. What ties every element together is a proactive approach to cybersecurity. Rather than wait for bad things to happen, the best kind of IT support anticipates issues and minimizes the potential damage from them.

That proactive approach is an important part of National Cybersecurity Awareness Month, too. As the "Secure Our World" digital toolkit states, "When IT providers and businesses work together, a safer digital future is possible for everyone."

Here are a few recommended tips as National Cybersecurity Awareness Month kicks off:

• **Strengthen passwords and implement multi-factor authentication (MFA).** According to CISA, "Passwords should be long, random, and unique to each account," and secure password managers should be used to generate and save them. But that one layer of security isn't enough—MFA is an enhanced protocol that adds a second element (like a verification code or identity confirmation) to any login attempt. This ensures that, even if a password is stolen, any attempt to compromise it can be mitigated.

• **Make sure software and hardware are updated and patched.** Out-of-date operating systems and expired applications can lead to serious security vulnerabilities. To better protect devices, data, and digital identities, make sure you install security updates and software patches with the assistance of a trusted IT provider. They can deploy these necessary updates during off-hours to minimize disruptions and digital threats.

• **Learn how to recognize and report phishing attempts.** Cybersecurity training empowers your employees to serve as the first line of defense. The key message, according to CISA, is to "Think before you click." Everyone in your organization should learn how to spot unsolicited emails, texts, or phone calls asking for sensitive information or personal details. Simulated phishing attempts can also train employees to spot questionable links before they click on them and avoid opening unknown attachments. Reporting these types of scams can also contribute to the knowledge necessary to identify and block them in the future.

• **Back up your data regularly, remotely, and redundantly**. No matter what threats your company faces, the best way to avoid bad outcomes from a ransomware attack or hack is with a reliable data backup. These should be executed automatically on a weekly (if not daily) basis and stored in multiple locations. In the event of an infection that encrypts or steals data, affected systems can be wiped clean and a recent backup can be used to restore data. That helps your business bounce back and return to regular day-to-day operations.

• **Explore multi-layered security tools.** Once the basics outlined above are in place, smart companies can work with their IT provider to consider more in-depth tools. These extra layers of defense protect against web-based attacks, block hidden bots that track keyboard activity, quarantine questionable email attachments before they land in your inbox, outline incident response protocols, and implement endpoint detection and response (EDR).

Special Topics for this Job: _____

_____

MSDS # _____ **Reviewed – Title:** _____

Present at Meeting:

_____ _____ _____

_____ _____ _____

_____ _____ _____

_____ _____ _____

Supervisor's Signature: _____

Note: These SAFETY TIPS OF THE WEEK are to help members provide a safe workplace and to instruct employees in ways to prevent accidents. Ensure you record the names of those who attend your safety meetings and file this form with your permanent accident prevention records.

SAFETY TIP OF THE WEEK

FOR THE CONSTRUCTION INDUSTRY

Company _____ **Date** _____

To encourage all of us to promote safety on a continuing basis, the Builders Exchange publishes a safety tip in each issue of the weekly Bulletin. The superintendent/foreman of each job should use this safety tip in a short safety meeting Monday morning. We suggest that this 5-to-10 minute meeting be just before lunch or perhaps right after the morning break. You can then emphasize the SAFETY TIP OF THE WEEK all week long.

Mes de Concientización sobre la Ciberseguridad

Week Ending 10/20/2023

Octubre es el Mes Nacional de Concientización sobre la Ciberseguridad, y 2023 marca el vigésimo aniversario del evento conmemorativo. El tema de este año es "Secure Our World", una campaña de servicio público creada por la Agencia de Seguridad de Ciberseguridad e Infraestructura (CISA) a instancias del Congreso de los Estados Unidos.

Con las amenazas digitales en aumento y el aumento de la complejidad de TI, es más que un simple eslogan: "Secure Our World" se trata de alentar a las personas y empresas a adoptar mejores hábitos de ciberseguridad y mejorar el comportamiento en línea.

Esto representa la oportunidad perfecta para evaluar el estado de la protección de su empresa. Para la mayoría de las empresas, eso comienza con una evaluación realista de los mayores riesgos actuales: ransomware, ataques de phishing y violaciones de datos. Estas tácticas son cada vez más comunes y pueden afectar negativamente a cualquier organización, grande o pequeña, en cualquier industria, ubicada en cualquier lugar de América del Norte. Por lo tanto, es imperativo abordarlos primero.

Pero la protección integral de la ciberseguridad se extiende mucho más allá, abarcando la copia de seguridad de datos, la gestión de identidades, las protecciones de inicio de sesión y la capacitación en el mundo real. Lo que une cada elemento es un enfoque proactivo de la ciberseguridad. En lugar de esperar a que sucedan cosas malas, el mejor tipo de soporte de TI anticipa los problemas y minimiza el daño potencial de ellos.

Ese enfoque proactivo también es una parte importante del Mes Nacional de Concientización sobre la Ciberseguridad. Como dice el kit de herramientas digitales "Secure Our World", "Cuando los proveedores de TI y las empresas trabajan juntos, un futuro digital más seguro es posible para todos".

Aquí hay algunos consejos recomendados a medida que comienza el Mes Nacional de Concientización sobre la Ciberseguridad:

• **Fortalezca las contraseñas e implemente la autenticación multifactor (MFA).** Según CISA, "las contraseñas deben ser largas, aleatorias y únicas para cada cuenta", y se deben usar administradores de contraseñas seguras para generarlas y guardarlas. Pero esa capa de seguridad no es suficiente: MFA es un protocolo mejorado que agrega un segundo elemento (como un código de verificación o confirmación de identidad) a cualquier intento de inicio de sesión. Esto garantiza que, incluso si se roba una contraseña, cualquier intento de comprometerla puede mitigarse.

• **Asegúrese de que el software y el hardware estén actualizados y parcheados.** Los sistemas operativos obsoletos y las aplicaciones caducadas pueden provocar graves vulnerabilidades de seguridad. Para proteger mejor los dispositivos, los datos y las identidades digitales, asegúrese de instalar actualizaciones de seguridad y parches de software con la ayuda de un proveedor de TI de confianza. Pueden implementar estas actualizaciones necesarias fuera del horario laboral para minimizar las interrupciones y las amenazas digitales.

• **Aprenda a reconocer y reportar intentos de phishing.** La capacitación en ciberseguridad permite a sus empleados servir como la primera línea de defensa. El mensaje clave, según CISA, es "Piensa antes de hacer clic". Todos en su organización deben aprender a detectar correos electrónicos, mensajes de texto o llamadas telefónicas no solicitados que solicitan información confidencial o detalles personales. Los intentos de phishing simulados también pueden capacitar a los empleados para detectar enlaces cuestionables antes de hacer clic en ellos y evitar abrir archivos adjuntos desconocidos. Denunciar este tipo de estafas también puede contribuir al conocimiento necesario para identificarlas y bloquearlas en el futuro.

• **Haga una copia de seguridad de sus datos de forma regular, remota y redundante**. No importa qué amenazas enfrente su empresa, la mejor manera de evitar los malos resultados de un ataque de ransomware o pirateo es con una copia de seguridad de datos confiable. Estos deben ejecutarse automáticamente semanalmente (si no diariamente) y almacenarse en múltiples ubicaciones. En el caso de una infección que cifra o roba datos, los sistemas afectados se pueden borrar y se puede utilizar una copia de seguridad reciente para restaurar los datos. Eso ayuda a su negocio a recuperarse y volver a las operaciones diarias regulares.

• **Explore herramientas de seguridad de múltiples capas.** Una vez que se hayan implementado los conceptos básicos descritos anteriormente, las empresas inteligentes pueden trabajar con su proveedor de TI para considerar herramientas más detalladas. Estas capas adicionales de defensa protegen contra ataques basados en web, bloquean bots ocultos que rastrean la actividad del teclado, ponen en cuarentena archivos adjuntos de correo electrónico cuestionables antes de que lleguen a su bandeja de entrada, describen protocolos de respuesta a incidentes e implementan detección y respuesta de puntos finales (EDR).

Special Topics for this Job: _____

_____

MSDS # _____ **Reviewed – Title:** _____

Present at Meeting:

_____ _____ _____

_____ _____ _____

_____ _____ _____

_____ _____ _____

Supervisor's Signature: _____

Note: These SAFETY TIPS OF THE WEEK are to help members provide a safe workplace and to instruct employees in ways to prevent accidents. Ensure you record the names of those who attend your safety meetings and file this form with your permanent accident prevention records.