Cyber-Safety for Physical Workers

A worker starts a shift, signs into a shared tablet, scans a QR code beside a machine, receives a text from someone claiming to be a supervisor, connects a diagnostic laptop to production equipment and uses a badge-controlled door before lunch. None of those actions looks like traditional occupational safety. Every one of them can now affect it.

The line between the digital workplace and the physical workplace has largely disappeared. Manufacturing systems, building controls, fleet technology, access systems, maintenance tools, sensors, mobile devices and industrial equipment increasingly depend on networks and software. That means a cyber incident can do more than expose information. It can interrupt production, remove visibility, disable access to systems, change operating conditions or force work into unfamiliar manual modes.

For years, cybersecurity awareness was treated as office training. Employees were taught not to click suspicious email links, reuse passwords or download unknown attachments. Those lessons still matter, but the audience is now much larger. Production workers, drivers, technicians, supervisors, contractors, warehouse employees and field crews interact with connected systems every day. They need enough cyber-safety knowledge to protect themselves, the operation and the people working around them.

That does not mean turning every worker into an IT specialist. It means adding a new category of hazard recognition to safety orientation: how to recognize when a digital event may create a physical or operational risk, what not to do, and how to report it before a small anomaly becomes a larger incident.

A practical starting point
SafetyNow offers a 30-course Internet Security Awareness Training package covering phishing, passwords, malware, cloud hygiene, remote work, AI-assisted scams and emerging cyber threats. The courses are designed as short, practical lessons that can be assigned and tracked through the LMS.
Explore SafetyNow Internet Security Awareness Training

The cyber-physical boundary has disappeared

Operational technology, or OT, is the hardware and software used to monitor or control physical processes. It includes systems such as programmable logic controllers, industrial control systems, building management systems, human-machine interfaces and other devices that can directly influence the physical environment. NIST’s Guide to Operational Technology Security emphasizes that OT security has to account for performance, reliability and safety, not just confidentiality of information.

The consequences are not theoretical. In July 2026, the FBI and EPA warned that malicious actors were targeting internet-facing programmable logic controllers used by water and wastewater utilities. The agencies reported incidents in at least seven U.S. states, with some activity degrading water operations after attackers changed device settings and caused loss of monitoring and control functionality. CISA issued a related alert urging operators to protect exposed OT devices.

The Canadian Centre for Cyber Security reaches the same broader conclusion. Its National Cyber Threat Assessment 2025-2026 identifies ransomware as the leading cybercrime threat to Canadian critical infrastructure and warns that disruption of critical services can put physical safety at risk. Its operational technology guidance also recognizes that cyber events can interfere with systems that monitor and change processes in the physical world.

Those examples involve critical infrastructure, but the principle applies much more broadly. A ransomware incident that shuts down a warehouse management system can change traffic flows and create rushed manual work. A compromised access-control system can affect who enters a restricted area. A malicious or corrupted update on a maintenance laptop can create an unexpected equipment problem. A lost work phone can expose credentials used to access other systems. An attacker who steals a supervisor’s account can send instructions that look legitimate to employees who have been trained to follow that supervisor’s messages.

Cyber risk therefore belongs in the same conversation as other changing workplace risks. Workers do not need to understand how the attack works in technical detail. They need to recognize the conditions under which the digital system can no longer be assumed to be trustworthy.

Why safety orientation is the right place

Safety orientation is where organizations teach workers how the workplace expects them to behave when conditions are normal and when something is wrong. New workers learn who can authorize work, which hazards require special controls, what must be reported, where emergency procedures are located and when they are expected to stop rather than improvise.

Cyber-safety fits naturally into that framework because many cyber incidents begin as a decision by an ordinary employee. The FBI notes that ransomware can be downloaded through malicious attachments, links and compromised websites. CISA specifically recommends training employees to recognize phishing, and its Cybersecurity Performance Goals call for basic cybersecurity training for employees and contractors. Canada’s Cyber Centre similarly recommends tailored employee training on phishing and suspicious links as part of ransomware prevention.

The important word is tailored. A forklift operator does not need the same cybersecurity orientation as a system administrator. A maintenance technician who connects laptops and removable media to equipment has a different exposure than a driver using a dispatch app. A supervisor who receives requests for employee data has a different decision profile than a contractor using a temporary site account.

Safety orientation gives employers a chance to teach the cyber behaviours that matter for each role before unsafe habits form. It also establishes something that annual cybersecurity modules often miss: the connection between a digital action and the worker’s own physical workplace.

The field worker is already part of the attack surface

Cybersecurity discussions sometimes describe employees as the ‘weakest link.’ That framing is not especially useful for safety training. Safety professionals learned long ago that blaming the last person who touched a system rarely explains why an

event occurred. People work inside procedures, technology, production pressures and organizational norms. Cyber-safety should use the same systems thinking.

Workers should be treated as an active layer of detection and response. They are often the first people to notice that a device is behaving differently, an expected screen has changed, a supplier request is unusual, a login prompt looks wrong or equipment is not responding as expected. The objective is to give them enough context to recognize those signals and a reporting path that does not punish them for raising a concern.

Phishing has moved beyond office email

A production worker may receive a fake payroll text, a driver may get a malicious delivery message, or a supervisor may receive a convincing request to open an invoice. Modern phishing can arrive through email, SMS, collaboration platforms, QR codes and social media. AI-generated content also makes spelling mistakes and awkward phrasing less reliable as warning signs.

Shared devices create shared exposure

Tablets, kiosks, handheld scanners and control-room workstations are often used by multiple people. Workers need rules for signing in and out, protecting credentials, responding to unexpected authentication prompts and reporting a device that has been lost or appears altered.

Removable media can reach equipment

USB drives and other removable media can be convenient ways to move files, updates and diagnostic information. CISA’s current performance goals recommend policies that prevent unauthorized media and hardware from being connected to IT and OT assets. Workers need to know that “just plugging it in” is a security decision.

Maintenance access can become a bridge

Technicians and vendors may use laptops, remote tools and diagnostic applications that connect directly to machinery or control systems. A legitimate maintenance task can become a pathway between environments if the device, software or account is compromised.

Physical access and digital access now overlap

Badges, smart locks, cameras and visitor systems are digital systems controlling physical space. Tailgating, lending credentials or approving an unexpected access request can create both security and safety exposure.

Operational anomalies may be cyber signals

Unexpected resets, missing alarms, altered settings, unusual login messages or a sudden loss of monitoring may have many causes. The worker does not need to diagnose whether the cause is cyber, mechanical or human. The safe response is to follow established operating and safe-state procedures and report the anomaly through the correct channel.

What cybersecurity training often gets wrong for physical workers

A conventional awareness program can technically cover every employee and still fail to prepare the workforce that operates the business. Four design mistakes are particularly common.

It uses office-only examples

If every scenario involves a laptop, an email inbox and a fake invoice, a warehouse worker or technician may reasonably conclude that cybersecurity belongs to someone else. Training should include the devices and decisions the target workforce actually encounters: scanners, tablets, QR codes, shared workstations, access badges, maintenance laptops, fleet applications and equipment interfaces.

It treats awareness as memorization

Definitions of phishing, malware and ransomware are useful, but safe behaviour depends on judgment. Workers need to practise deciding what to do when the request appears plausible, when production is waiting, when the person asking seems senior, or when the normal digital process has stopped working.

It punishes mistakes instead of improving reporting

A worker who realizes they clicked a suspicious link should report it immediately. If the organization’s culture teaches people that reporting a mistake will lead to embarrassment or punishment, the organization may lose the minutes that matter most for containment. Cyber-safety reporting should borrow from effective near-miss programs: reward early reporting and learn from the conditions that made the action seem reasonable.

It separates IT security from operational safety

Information technology teams may understand the digital threat, while operations and safety teams understand how loss of a system changes the physical work. Effective preparation requires both perspectives. Cybersecurity controls should not be designed without considering how workers will operate when systems are unavailable, and safety procedures should not assume that digital information will always be accurate or accessible.

The PAUSE standard for cyber-safe work

A safety orientation needs a simple behavioural standard workers can remember when the situation is ambiguous. PAUSE provides five actions that apply across roles without expecting employees to diagnose the technology.

PAUSE	Worker behaviour	Why it matters
P — Pause	Stop before clicking, scanning, connecting, approving or bypassing when something is unexpected.	Time pressure is a common ingredient in social engineering and unsafe workarounds.
A — Authenticate	Verify unusual requests through an approved, separate channel.	A convincing message or familiar name is not proof of identity.
U — Use approved tools	Use authorized devices, media, applications, networks and accounts.	Unapproved tools can introduce malware, expose credentials or bypass controls.
S — Speak up	Report suspicious messages, lost devices, strange prompts and unusual system behaviour quickly.	Early reporting gives IT, security and operations more time to contain an event.

PAUSE	Worker behaviour	Why it matters
E — Escalate safely	If a digital problem affects equipment or the process, follow established safe-state and emergency procedures. Do not improvise around a safety control.	A cyber problem becomes a safety problem when workers compensate for lost visibility or control in unsafe ways.

PAUSE is intentionally simple. It does not replace an organization’s cybersecurity policies, OT procedures or emergency plans. It gives workers a common response when a digital event feels unusual and the correct technical answer is not obvious.

What every physical worker should learn in orientation

A useful cyber-safety segment can be short if it is specific. The objective is not to cover the entire threat landscape on day one. It is to establish the behaviours that reduce immediate exposure and create a foundation for ongoing awareness training.

Why cyber belongs in safety

Explain in plain language that connected devices can affect production, access, communication and physical processes. Workers should understand why a suspicious digital event is relevant to their job.

Which devices and systems they are authorized to use

Show employees which phones, tablets, kiosks, scanners, workstations, networks, USB devices and accounts are approved. Avoid expecting them to infer the rules.

How to recognize suspicious requests

Teach urgency, unusual payment or credential requests, unexpected MFA prompts, impersonation, new QR codes, unrequested attachments and requests to bypass normal procedures.

How credentials are protected

Cover unique passphrases, MFA, password managers where used, account sharing prohibitions and why badges or access codes should not be loaned.

What not to connect

Explain the organization’s rules for USB drives, personal devices, chargers with data capability, diagnostic equipment and vendor laptops.

What digital anomalies to report

Workers should report unexpected screens, changed settings, disabled alarms, repeated resets, unusual access events, suspicious pop-ups, unfamiliar software or unexpected requests for credentials.

What to do after a suspected mistake

Tell workers exactly who to contact if they clicked, scanned, downloaded, shared credentials or lost a device. The message should be immediate reporting, not concealment.

How to respond when technology fails

Reinforce the approved manual, safe-state, shutdown or emergency procedure. A digital

outage is not permission to bypass an interlock, alarm, authorization step or other safety control.

Build the awareness layer before the incident
SafetyNow's Internet Security Awareness Training package includes 30 courses covering email threats, passwords, malware, response to malware, cloud hygiene, remote work, AI-generated deception, emerging cyber threats and more. Organizations can assign training, monitor participation and retain completion records through the LMS.
View the 30-course package and request a demo

Five scenarios that make cyber-safety real

Orientation becomes more useful when workers practise decisions instead of listening to definitions. These scenarios can be adapted to the organization's own roles and systems.

1. The maintenance update

A technician receives a USB drive from a vendor who says it contains an urgent firmware update needed to restart a machine. Production is waiting. The correct discussion is not whether USB drives are always unsafe. It is whether this media and update have been verified and approved through the organization's maintenance and cybersecurity process.

2. The supervisor text

A worker receives a text that appears to come from a supervisor asking them to sign into a scheduling page because the shift has changed. The link opens a familiar-looking login screen. The worker should pause and verify the request through an approved channel rather than using the link.

3. The new QR code

A QR code has been placed beside a piece of equipment and claims to link to the latest procedure. The worker has never seen it before. The lesson is to use approved sources for procedures and report unexpected signage or links rather than assuming physical placement makes them legitimate.

4. The strange HMI

An operator notices that an expected alarm is missing and several values briefly freeze. The equipment continues to run. The worker should follow the organization's established operating and escalation procedure, avoid bypassing safeguards, and report the digital anomaly as part of the event.

5. The lost shared tablet

A team cannot find a tablet used for inspections and equipment checklists. Someone suggests waiting until the end of the shift to see whether it turns up. The correct action is immediate reporting so access can be protected and the device can be managed according to company policy.

Cyber incident response is also a safety issue

Most cyber incident plans are written for IT, security and leadership. Physical workers also need a small, clearly defined role. Canada's Cyber Centre recommends that organizations develop employee training so people understand their roles, responsibilities and the order of operations during a ransomware incident. That principle matters because operational confusion can create secondary hazards even

when the cyber event itself did not directly manipulate equipment.

A system outage may remove access to work orders, permits, procedures, drawings, emergency contacts, inventory records or maintenance history. Employees may be tempted to use screenshots, personal devices, old printed copies or improvised communication channels. Some work can continue safely under approved contingency procedures. Other work should stop until the required information or control is restored.

The orientation message should therefore be explicit: when a cyber or technology event affects a safety-critical system, employees follow the organization's established safe-state, shutdown, business-continuity or emergency procedure. They should not reset, reconnect, bypass, reconfigure or substitute systems unless their role and procedure specifically authorize them to do so.

This is the same principle used in high-quality safety programs generally. Uncertainty should trigger a controlled response, not improvisation. Cybersecurity becomes occupational safety when the loss of trusted information or control changes what workers can safely do.

Role-based cyber-safety beats generic annual awareness

NIST's OT security guidance recommends cybersecurity training relevant to the OT environment for employees, contractors, consultants and vendors, in addition to general IT awareness. That is an important distinction for employers with physical operations. Everyone needs a common baseline, but exposure varies by job.

Role	Likely cyber-safety exposure	Training emphasis
Production operator	Shared workstations, HMIs, production tablets, unexpected system behaviour	Account protection, anomaly reporting, approved recovery procedures, no bypassing
Maintenance technician	Diagnostic laptops, USB media, vendor tools, remote access, firmware and software	Approved devices and media, update verification, vendor access, escalation
Driver or field worker	Mobile devices, dispatch apps, text messages, public networks, QR codes	Smishing, device loss, MFA, approved connections, reporting
Supervisor	Approvals, employee data, invoices, schedule changes, emergency communications	Impersonation, BEC, verification, escalation, reinforcing reporting culture
Contractor or temporary worker	Temporary accounts, site Wi-Fi, access badges, unfamiliar devices and procedures	Site-specific cyber rules, account boundaries, access control, reporting contacts

Do not turn awareness training into the cyber control

Cyber-safety training matters, but it cannot compensate for weak technical controls. A worker should not be expected to detect every malicious message or protect an internet-exposed industrial controller through good judgment alone. CISA, NIST and the Canadian Cyber Centre consistently pair workforce awareness with technical measures such as MFA, strong authentication, network segmentation, patching, access control, backups, secure configuration and protection of OT from unnecessary internet exposure.

This matters for safety leaders because organizations sometimes respond to an incident by assigning more training when the underlying problem is architectural. If a worker can connect unauthorized media directly to a safety-critical system, the answer may include training, but it should also include technical restrictions. If shared passwords are operationally necessary because individual accounts were never provisioned, the problem is not simply worker behaviour. If employees routinely bypass a slow approval process to keep production moving, the system is teaching the shortcut.

The best programs use training to support controls rather than substitute for them. Workers learn what the controls are designed to protect, how to use them correctly and how to respond when they appear to fail.

How SafetyNow can support the cyber-safety layer

For many employers, the hardest part is not deciding that cybersecurity awareness matters. It is delivering enough practical training to a workforce that already has required safety, compliance, equipment and operational training competing for attention.

SafetyNow's Internet Security Awareness Training package is designed to make that layer easier to deploy. The current package includes 30 courses across common cyber risks, with short lessons intended to build practical judgment. Topics include phishing and impersonation, stronger passwords and MFA, malware and ransomware, cloud and collaboration hygiene, remote work, AI-generated deception, emerging threats, safe browsing, social engineering, device protection and privacy.

The platform also addresses the management side of the problem. Organizations can assign training, monitor participation and completion, retain certificates and use centralized reporting rather than relying on informal reminders or disconnected training files. Mobile-ready delivery also makes the program usable by employees who do not spend their day at a desk.

The most effective implementation is not to assign all 30 courses to every employee at once. Build a baseline, then use role and exposure to sequence the learning. A field crew may begin with phishing, passwords, mobile-device security and social engineering. Maintenance may add malware, device security and emerging threats. Supervisors may receive additional emphasis on impersonation, business email compromise and approval fraud.

Organizations can review the package and register for discount pricing or a demonstration at **SafetyNow Internet Security Awareness Training**.

A 30-day plan to add cyber-safety to orientation

Organizations do not need a year-long cybersecurity transformation to improve orientation. A focused 30-day project can establish the workforce layer while IT and security teams continue strengthening technical controls.

Week 1 — Map the cyber-physical touchpoints

- List the devices and digital systems physical workers use or depend on.
- Identify roles that connect removable media, maintenance laptops or vendor tools.
- Identify safety-critical information that would be affected by a system outage.
- Review how workers currently report suspicious digital activity or technology failures.
- Ask where production pressure is most likely to encourage an unsafe workaround.

Week 2 — Build the orientation module

- Explain the connection between cyber events and physical operations.
- Teach the PAUSE standard using examples from the actual workplace.
- Show approved devices, networks, apps, login practices and reporting channels.
- Include at least two role-specific decision scenarios.
- Clarify what workers should do if a digital system affects safe operation.

Week 3 — Train supervisors and response owners

- Give supervisors a consistent way to respond when workers report mistakes or suspicious events.
- Confirm who receives reports after hours and during production emergencies.
- Make sure safety, operations and IT understand who owns each type of response.
- Test an alternate communication method if normal systems are unavailable.

Week 4 — Launch, reinforce and measure

- Add the cyber-safety segment to new-hire and contractor orientation.
- Assign baseline Internet Security Awareness Training to the appropriate roles.
- Reinforce one cyber-safety behaviour in toolbox talks or supervisor meetings.
- Run a short scenario and measure whether workers choose the correct response.
- Review reporting data and refine the orientation based on what employees find confusing.

Measure judgment, reporting and recovery readiness

Completion rates still matter because employers need to know who received required awareness training. They are not enough to determine whether the workforce can respond safely. A stronger measurement set combines participation with decision quality and reporting behaviour.

- Percentage of targeted workers who completed baseline and role-specific training.
- Performance on realistic scenarios rather than definition-only quizzes.
- Whether employees know exactly how and where to report a suspected incident.
- Time between recognizing a suspicious event and reporting it during exercises.
- Number and quality of real suspicious-message, device-loss and anomaly reports.
- Repeated problem areas, such as shared credentials or unapproved media, that indicate a process or technical-control issue.
- Results of tabletop exercises involving loss of a safety-critical digital system.
- Whether supervisors respond consistently and avoid discouraging early reporting.

Be cautious about treating a simulated-phishing click rate as a complete measure of cyber readiness. It may be one useful signal, but message difficulty, context and workforce conditions affect the result. The more important question for a safety-oriented program is whether people recognize risk, report quickly and know how to keep the physical operation safe when digital trust is uncertain.

Cyber-safety is becoming part of ordinary safety competence

The physical worker of 2026 is also a digital worker, even if they never sit in an office. The scanner in a warehouse, tablet in a truck, badge at a gate, HMI on a production line and diagnostic laptop beside a machine are all part of a connected operating environment. The worker does not need to administer those systems to affect their security.

That changes what good orientation looks like. Employers still need to teach lockout,

PPE, emergency procedures, hazard reporting and the controls associated with the job. They should now add the digital behaviours that protect those same systems and people: verify unexpected requests, protect access, use approved tools, report anomalies and never improvise around a safety control because technology is unavailable.

Cybersecurity teams cannot solve that problem alone because they are not standing beside every machine, vehicle, loading dock or field crew. Safety and operations teams cannot solve it alone because the threat may be invisible until it appears through technology. The workforce connects the two worlds.

The goal is not to make workers afraid of technology. It is to give them the same confidence they should have with any other workplace hazard: know what normal looks like, recognize when something has changed, understand the limits of your authority, and report early enough for the organization to respond before exposure becomes loss.

Make cyber-safety part of the training system
SafetyNow’s 30-course Internet Security Awareness Training package helps organizations build practical awareness around phishing, ransomware, credentials, malware, AI-enabled scams and other current threats. Training is mobile-ready and can be assigned, tracked and documented through the SafetyNow LMS.
Get discount pricing and request a SafetyNow demo