



Cyber Hygiene for OT Installers

Securing BAS White Paper Series 1 of 6

CONTACT INFORMATION

877.444.5622 

info@kmccontrols.com 

www.kmccontrols.com 

19476 Industrial Drive, New Paris, IN 46553 



Table of Contents

Executive Summary 1

Introduction 1

What Is Cyber Hygiene? 2

How Social Engineering Works 2

A Real-World Cautionary Tale 3

Cyber Hygiene for OT Professionals: Do’s and Don’ts 3

Minimum Security Expectations on Every Job 4

What Owners and Service Providers Should Require 5

How Cyber Hygiene Complements Technical Security 5

Conclusion 6



Executive Summary

Even the most technically secure building automation system (BAS) can be compromised by a simple human error. This paper introduces the essential concepts of cyber hygiene for Operational technology (OT) installers and explains how phishing, impersonation, unsafe removable media, and weak credential practices can undermine connected building systems. It also adds an important operational point: awareness alone is not enough. Good cyber hygiene should be backed by approved remote access methods, unique accounts, documented changes, incident reporting, and coordination with both the system owner and service provider.

Introduction

OT installers historically focus on wiring, configuring, and troubleshooting BAS hardware, not defending against phishing emails or USB-based malware. However, as OT environments become more connected, installers increasingly find themselves in the crosshairs of cyber attackers.

Cyber hygiene is not just for corporate office workers. It is critical for anyone with access to connected devices, network credentials, service laptops, or remote access portals. This paper outlines the core concepts of cyber hygiene, shares lessons learned from high-profile breaches, and adds a few minimum expectations that help align installer behavior with owner requirements, service provider procedures, and secure system operation.

What Is Cyber Hygiene?

Cyber hygiene refers to routine behaviors and awareness practices that reduce the risk of security incidents. As physical hygiene prevents illness, cyber hygiene protects your devices, credentials, and networks from infection or misuse.

Key principles include:

- **Think before you click:** emails, links, and attachments are common attack vectors.
- **Verify before you trust:** attackers often impersonate people you know.
- **Do not plug in unknown devices:** USB sticks can instantly deliver malware.
- **Keep your systems tidy:** use strong passwords, updated software, secure your defaults, and use only approved service tools.
- **Secure physical access:** lock control panels, wiring closets, and service ports. Unauthorized physical access to OT devices can be just as damaging as a network breach.

In OT work, cyber hygiene also means using only approved remote connections, unique named accounts, scanned media, and documented site changes. These habits apply everywhere, not just in the office.

How Social Engineering Works

Social engineering is when attackers manipulate people into giving up access or information. It is not a technical exploit; it is a human one. Examples include:

- **Phishing:** An email pretends to be from a trusted source and asks you to click a link, download a file, or enter credentials.
- **Impersonation:** You get a text from your boss asking you to urgently buy gift cards because he “forgot his wallet.”
- **Baiting:** You find a USB thumb drive in the parking lot labeled “confidential.” Plugging it in could instantly compromise your laptop.

These tactics work because they exploit trust and urgency. The more connected OT systems become, the more valuable your credentials are to attackers.

A Real-World Cautionary Tale

When Target suffered a massive data breach in 2013, the attackers did not need to start inside a store controller. The breach began when an HVAC contractor employee clicked on a phishing link and the attackers gained access to the contractor's credentials for Target's vendor portal. The lesson for OT installers is clear: cyber hygiene matters at every layer of the supply chain, and vendor access should be governed with unique accounts, MFA, approvals, and fast reporting when something looks wrong.

Because OT contractors often work across multiple customer sites, one compromised account or unmanaged remote connection can create risk beyond a single project. This is why credential separation, access approval, and quick escalation are part of proper cyber hygiene.

Cyber Hygiene for OT Professionals: Do's and Don'ts

DO:

- ✓ Be suspicious of any message asking you to act quickly, especially if it involves money, passwords, or urgent access requests.
- ✓ Use strong, unique passwords for each system. Consider a password manager if your company allows it.
- ✓ Report suspicious emails, texts, malware warnings, or credential concerns to your company security lead, and, when customer systems may be affected, to the site owner or authorized representative.
- ✓ Confirm identity by calling the person directly if something seems off.
- ✓ Keep your work laptop and tools up to date; do not postpone security updates.
- ✓ Change default passwords on every device immediately upon installation, and record the change according to proper procedure.
- ✓ Use multi-factor authentication (MFA) for any remote access portals and connect, but only through owner-approved remote access methods.
- ✓ Remove temporary access when the work is complete.
- ✓ Use only approved and scanned USB media, and keep service laptops free of personal software and unknown files.
- ✓ Document installed devices, network changes, remote access enablement, and security-relevant settings

DON'T:

- ✗ Do not reuse passwords across job sites or systems.
- ✗ Do not connect unknown USB drives or devices.
- ✗ Do not click links in emails from senders you were not expecting, even when the message looks official.
- ✗ Do not trust a caller or texter just because they use your boss's name.
- ✗ Do not use the same credentials for a customer's system that you use for your own company systems, other job sites, or shared generic vendor accounts.
- ✗ Do not leave persistent remote access tunnels, modems, or support accounts enabled after commissioning unless the owner has explicitly approved them.
- ✗ Do not make unapproved configuration changes or leave changes undocumented.

Minimum Security Expectations on Every Job

Cyber hygiene is strongest when it is supported by a few simple management practices:

- **Access approval:** the owner or authorized service lead approves who connects, how they connect, and when they connect; sessions use MFA and are terminated when work is complete.
- **Account control:** use unique accounts, remove default credentials, prohibit password sharing, and keep credentials separated between customer sites.
- **Asset and change records:** document installed devices, IP changes, remote access settings, and security-relevant configuration changes.
- **Reporting and recovery:** report suspicious activity, lost devices, malware, or possible credential exposure immediately so response steps, logs, and backups can be used if needed.

What Owners and Service Providers Should Require

Installers are most effective when the surrounding program is equally disciplined. This paper is the human-behavior baseline; it does not replace documented owner policies or system security settings.

- Provide a named security or escalation contact before site work begins.
- Hold subcontractors to the same account, media, remote access, and reporting expectations as prime contractors.
- Log and review remote sessions, and disable access when it is no longer needed.
- Maintain asset inventories, network diagrams, and change records for BAS environments.
- Support the broader OT program with system logging, time sync, backups, and recovery planning.

How Cyber Hygiene Complements Technical Security

Securing BAS White Paper 3, Hardening BACnet Networks, describes how to secure BAS networks and devices using segmentation, access controls, and firewalls. However, these technical defenses can still be undermined by a single phishing click, a reused password, or an unmanaged vendor connection. Cyber hygiene is the human layer of defense, but it is not a substitute for governance. A mature OT program ties technician behavior to owner requirements, service-provider procedures, and system capabilities such as auditing, account management, boundary protection, backup, and recovery.

Conclusion

Cybersecurity is not just the IT team's job. As OT systems connect to broader networks, every installer, technician, and contractor becomes part of the security posture and influences credentials, remote access, physical access, and documentation quality. By practicing cyber hygiene and following approved access, account, reporting, and change-management practices, OT professionals help prevent the very attacks that make headlines and erode trust. Combined with technical best practices and IT/OT collaboration, proper cyber hygiene makes building systems safer, smarter, and more resilient.