REDLENS INFOSEC™

Visitor Management

Social engineering attacks don't only exist on your computer. By claiming to be an employee or vendor with official-looking credentials, criminals can coax information from employees or gain physical access to systems. Criminals have been known to steal or purchase old vendor uniforms as a way to bypass security or avoid scrutiny. They may pose as janitorial staff, IT employees there to “fix” something, or even auditors/consultants.

If sensitive information, like non-public information (NPI) or cardholder data (CHD) is present in the area, the following should be included in your visitor management procedures:

1. All visitors must be properly screened and authorized before allowing them entry. They should also be escorted at all times while onsite.
2. Approved visitors should be given a badge or other method of identification that distinguishes them from regular staff. Limitations and expiration dates should be placed on visitor badges, and you should require that they are returned upon exit.

3. Be mindful of “tail-gaiting” or unauthorized individuals trying to follow an authorized individual through a secure door without providing their own access card or code. Make sure employees also don’t allow someone claiming they left their badge at their desk to follow them in.

4. Ensure that employees are safeguarding their access cards and badges by not leaving them unattended on their desks or in unlocked cars in the parking lot.

5. A documented visitor log should be kept that details the visitor’s name, organization they are representing, and the onsite employee who granted them access. This log should be retained for at least 3 months, so it can be reviewed in the event that a device was discovered to have been tampered with or information had gone missing.

6. For highly sensitive areas, install cameras that record all individuals entering/exiting the area. You may also take photographs of visitors, or scan ID cards and driver licenses.

7. Review your visitor management procedures with staff as part of your ongoing security awareness training.

8. Enlist the help of third-party penetration testers to perform a physical pen test to analyze their ability to gain unauthorized access into your building through social engineering tactics or other techniques.

For additional guidance on protecting the security of your organization’s sensitive systems and information with an effective Visitor Management procedure, contact RedLens InfoSec.

REDLENS
INFOSEC™