



Mineral



Question of the Week

September 10, 2025

Question

What is a phishing scam and how can we protect our organization and employees?

ANSWER

Phishing is a scam in which the attacker pretends to be a trusted person or company and uses electronic means such as emails, texts, or phone calls to steal information. Specifically, the attacker tries to trick you into handing over sensitive information like usernames, passwords, payroll data, banking information, and customer data. They often encourage you to click a link, download an attachment, or provide information—sometimes by mimicking legitimate emails you would expect to receive. A successful phishing attack can be costly, in terms of both finances and your company's reputation.

To address this issue, your IT department will need time, funds, and resources. They'll likely want to take a multi-pronged approach that includes installing and updating software, training employees to recognize and report phishing attempts, creating a recovery plan, alerting the organization when there's an active phishing attack, and possibly simulating phishing attempts to test employees.

You can also protect your organization by establishing and enforcing strict processes for requesting and sending personal, sensitive, or confidential information. For instance, employees should know not to send you payroll information or login credentials over text or email.

This Q&A does not constitute legal advice and does not address state or local law.