Short Training Beats Long Lectures

Security awareness works best when it's **short, simple, and repeated often.**

Think about **seat belts in a car.**

Years ago, people forgot to wear them.
Now cars remind us every time we start the engine.
Security training works the same way.
Small reminders — delivered regularly — help employees build safer habits.
Short lessons, quick tips, and real examples keep security **top of mind.**

Build Your Human Firewall

Technology protects systems.
But **people protect businesses.**

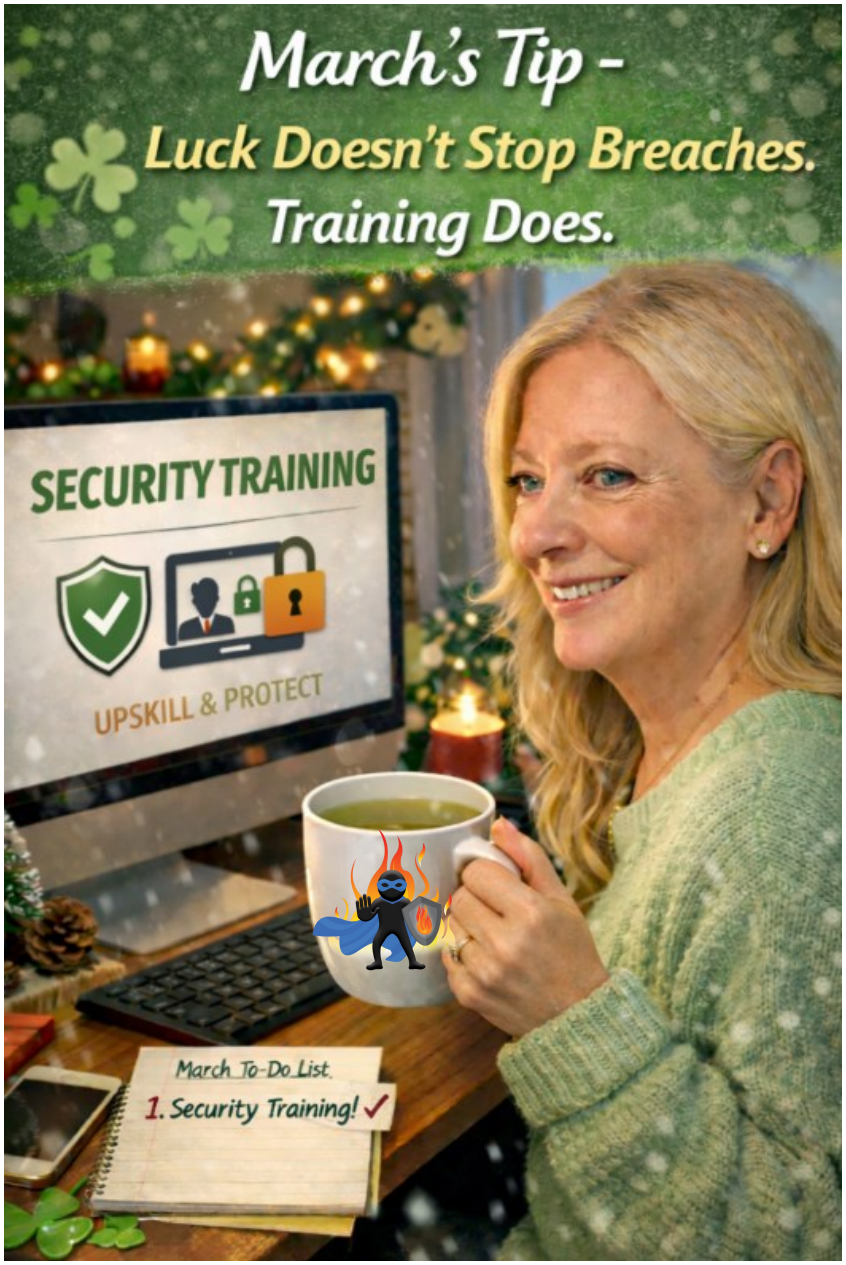
When employees receive ongoing security training, they learn to:

- Spot phishing messages
- Question unusual requests
- Protect passwords and accounts
- Report suspicious activity quickly

A well-trained team becomes a **Human Firewall** that helps stop cyberattacks before they start.
And that's far better than relying on luck.

ACT SMART I.T.
Helping You Benefit From Today's Technologies

332 Main Street, Wareham, MA 02571
781-826-9665 | 855-WOW-SERVICE
ACTSmartIT.com



Your 12 Month Cybersecurity Roadmap

Follow us each month at:
ACTSmartIT.com/2026-roadmap/

Security Awareness Training for Employees

Luck Doesn't Stop Breaches. Training Does.

Cybercriminals are always looking for the **easiest way into a business network**. Most of the time, that door isn't a server or firewall.
It's a person.

Employees receive emails, texts, and phone calls every day. Attackers know this and try to **trick people into clicking, downloading, or sharing information**.
That's why **security awareness training is one of the most powerful tools a company has.**
When employees know what to watch for, they become a **Human Firewall** that protects the business.

Humans Are the Front Door

Most cyberattacks don't start with complicated hacking.
They start with **a message designed to fool someone**.
Examples include:

• Fake password reset emails
• Messages pretending to be from a boss
• Fake invoices or payment requests
• Phone calls asking for account information

Attackers rely on **urgency, fear, or curiosity** to get people to act quickly without thinking.

A trained employee pauses and asks:
"Is this real?"

That one moment of caution can stop a breach.

Phishing: The #1 Attack Method

Phishing emails try to **trick users into clicking links, opening attachments, or entering passwords**.

Common signs of phishing include:

- Unexpected attachments
- Messages asking you to verify your password
- Links that don't match the sender
- Urgent requests for payment or gift cards
- Slightly misspelled company names

Even smart people fall for phishing sometimes. That's why **practice and reminders matter.**

Social Engineering: Manipulating People

Social engineering is when criminals **manipulate people instead of technology**.

Examples include:

- Someone calling and pretending to be IT support
- A message that appears to come from the CEO
- A delivery driver asking to "borrow" a computer login
- Someone entering an office behind an employee

Attackers count on people wanting to **be helpful and polite**.
Security training teaches employees when it's okay to say:
"Let me verify that first."

Real-World Scam Examples

These types of scams happen every day:

Fake Invoice Scam
A company receives an email that looks like it came from a vendor asking to update payment information. The payment goes to a criminal instead.

CEO Fraud
An employee receives an urgent email from "the boss" asking them to purchase gift cards or transfer money.

Password Reset Scam
A message claims your account was locked and asks you to log in to fix it — but the page steals your password.

These scams succeed when people **haven't seen them before.**