SEV1TECH MANAGED SERVICES

12700 Black Forest Ln, Suite 205, Woodbridge, VA 22192
Telephone: (703) 496-3776 | Fax: (703) 496-3797
sev1tech.com

End User Security Platform

What is the greatest risk to your business?

Why Us

In a world full of technology, criminals constantly lurk behind screens and fake emails waiting for their next victim to click a link they're not supposed to. It's up to you to decide whether you are going to let them win. Cyber Security is crucial, but what's even more valuable is having an educated fleet of employees that have a deep understanding of *why* it is crucial. Here at Sev1Tech, we believe teaching the "why" in cyber security will create a human firewall making your company resilient to malicious attacks.

Create Your Human Firewall

Keeping your staff trained in security basics, ongoing threats, scams to watch out for, and how to protect your business has never been easier. Let us do the heavy lifting in training your employees by feeding them easy-to-read, digestible information that will prevent your greatest asset -humans- from being your greatest risk.

53%

of cyber attacks are due to

Human Error

Dark Web Scanning

Proactively monitor the dark web for compromised account data for up to 3 company domains. We also provide users the ability to scan the dark web for personal accounts as well.

Phishing Campaigns

Routine simulated phishing has been proven to minimize the risk of end-users falling victim to a malicious phishing attempt.

Weekly Micro-Training

2-4 minute video training sent weekly with multiple choice quiz questions to keep users continuously training while enhancing their Employee Security Score (ESS)

Basic Cybersecurity Policy Generation

Policies and procedures are key to establishing expectations. Our document management portal contains a variety of customizable security policies.

Baseline Employee Cybersecurity Assessment

A baseline first test for your employees. Gauge their cybersecurity knowledge across 6 topics including phishing awareness, handling PII, social media, and working remotely.

Periodic Reviews of Cyber Hygiene

Set the standard throughout the year with an overview and assessment of the most important cybersecurity practices.

Fast Facts

What is the dark web?

- The dark web is a dangerous part of the internet that lets users remain untraceable so that they can execute illegal activity without the risk of getting caught. The dark web is home to millions of people buying and selling drugs, guns, counterfeit money, stolen subscription credentials, and other private information breaching others' security.

Common cyber security threats

- **Phishing:** the fraudulent practice of sending emails or other messages purporting to be from reputable companies to convince individuals to reveal personal information, such as passwords and credit card numbers.
- **Spoofing:** when scammers deliberately falsify the information sent to your caller ID to disguise their identity.
- **Ransomware:** a disguised, executable that encrypts files from a database. This software then forces companies to pay set amounts of money to recover the breached data.

Why Cyber Security Matters to You

- The number one threat to a company's day-to-day functions comes from the web. Whether it be email, browsing the web, or downloading and installing software.

Did you know?

- The average cost to completely recover from a data breach is currently $4.35 million.

What Can We Do?

You wouldn't expect employees to know how to respond to an emergency if you didn't have emergency drills…

5%

Susceptibility rates have dropped to as low as 5 percent when employees are well-trained and phished.

Frequent simulated social engineering testing + Security Awareness Training + Commitment & C-level buy-in = **DECREASED SUSCEPTIBILITY**

40%

Real-time phishing simulations have proven to yield a near **40% ROI**

Let's Chat

To begin your security journey with Sev1Tech, contact one of our MSP experts at msp-sales@sev1tech.com.

SEV1TECH MANAGED SERVICES