October 2025 | CSN-Q4-2025

Leading security practices for small businesses.

Securing Your Email Domain

Summary

Running your small business is like conducting a symphony orchestra – lots of moving pieces working together to make beautiful music come to life.

Your customers seek you for your products and services through many channels – phone calls, the internet, and email.

Your financial institution wants you to be aware of a security threat that you may be facing, but be unaware of, and it involves securing your email domain from misuse.

Email Breach Statistics

- Email breaches are highly prevalent, with phishing attacks accounting for a significant portion of cyber threats.
- 75% of targeted cyberattacks start with an email, while 44% of social engineering incidents involve phishing specifically.
- 94% of malware is delivered via email attachments, and attacks like Business Email Compromise (BEC) are the primary vector for data breaches in some sectors.

\- *Keepnet Labs*

How it Works

Imagine the threat actor tricking an employee into clicking on a link or opening an attachment, then breaking into their email account using a stolen username and password.

The stealthy actor lies in wait, creates a rule to prevent detection, and accumulates information about your business, your customers, and financial information.

Finally, the actor impersonates staff and customers to commit financial fraud, including business email compromise, account takeover, and CEO fraud.

What makes detection so difficult is its subtlety, because people are naturally trusting, and there is an expectation that the business has controls in place to prevent such things from occurring.

What's Your Risk?

A thorough risk assessment helps you to identify your risk from of following areas:

Operational Disruption. Business interruption and downtime divert time and energy from servicing customers (e.g., ransomware incidents prohibit access to stored data unless a ransom is paid), data corruption, business restoration costs, supply chain issues, loss of revenue, and similar consequences.

Reputational Damage. Following a disclosed breach, information that becomes public knowledge can diminish your reputation and reduce consumer confidence.

Financial Loss. Breach remediation costs may vary; however, they are substantial. For example, the average cost for a data breach in the US was $9.4 million in 2023, while the global average was around $4.88 million in 2024. Your competitive advantage may be adversely affected.

Legal & Regulatory Costs. If your business fails to protect sensitive information (such as HIPAA, GDPR, and GLBA) in your email servers, you may face legal action for non-compliance. Additionally, you may also face lawsuits from victims of the incident.

Reducing Your Business's Risk

It doesn't matter what the size of your business is; good cyber hygiene, training, and reporting processes will reduce your risk because the consequences are too great. Whether you outsource your information technology service or manage it internally, here are some basic tips to reduce your risk.

- √ Utilize Multi-Factor Authentication wherever possible
- √ Continuously update anti-virus and other critical software to prevent new exploits.
- √ Perform regular security audits to proactively identify and remediate defense weaknesses.
- √ Ongoing threat monitoring to detect unusual activity in real time within and outside of your network to identify and block unauthorized access attempts.

! If you detect that you've had a security compromise, immediately notify your financial institution.

Resources

- Enhance Email & Web Security
- Microsoft 365 for business security best practices

What to Do if You Are Scammed

- Contact your financial institution immediately so they can act and provide recommendations.
- Keep detailed records and document all communication, actions taken, and the timeline of events.
- Identify and secure systems by examining communication channels (emails, phone calls) for any signs of phishing or unauthorized access.
- If you are the victim of burglary, vandalism, or theft, contact your local law enforcement agency.
- If your Social Security or individual tax identification number was stolen, immediately report it to IdentityTheft.gov.

- Report suspicious activity to the Internet Crime Center, www.ic3.gov, and/or your local law enforcement agency.

12120 Sunset Hills Rd, Reston
VA 20190