SCANTRON
TECHNOLOGY SOLUTIONS

SMART STARTS HERE

Cybersecurity Tips

Keeping Your Systems Safe

Scantron is a firm believer in setting standards and being proactive when it comes to cybersecurity threats. With news and information being disseminated over possible foreign threats, we have actively taken measures to ensure the security of Scantron networks. Scantron follows Department of Homeland Security (DHS) recommendations and is attentive to any new threats that may emerge.

Q1

64%

Companies who don't know their organization's endpoints

I know what devices are on my network

One of the best ways to protect your environment is to know what devices have access to your network—and whether they should.

Q2

40%

Companies who don't use HTTPS as their default website protocol

I know the hardening standards of my devices

Make sure devices are hardened against attack. Know what the recommended standards are and follow industry best practices.

Q3

279

Avg number of days it takes to identify and contain a breach

My response plans cover cybersecurity events.

Ensure you have a response plan to rapidly identify and address an attack. Test your plan periodically, and update it as new threats emerge.

Q4

94%

Share of malware delivered via email

I know the common cybersecurity threats to my devices.

Phishing, malware, ransomware—attacks can come from many directions. Ensure you and your team know how to spot intrusions.

Q5

$3.92 Million

Avg total cost of a data breach

I know the impact of a cybersecurity incident to my business.

It's only a matter of time until you experience a cyberattack. The impact can be significant, so make sure you're prepared.

7 Steps You Can Take Today to Increase Cybersecurity

1. ***Train staff***
   - To identify phishing emails
   - To be aware of key ransomware identifiers:
     - › Applications, attachments, or both in emails requesting permissions not normally required, such as logging in prior to using.
     - › Duplicate files of the same name and type with different extension endings.
2. ***Enhance/harden email server settings***
   - Sender Policy Framework (SPF)
   - DomainKeys Identified Mail (DKIM)
   - Domain-based Message Authentication Reporting and Conformance (DMARC)
3. ***Acquire and use a SIEM (Security Information and Event Manager)***
   - Real-time analysis of application and network device alerts.
   - Regularly scheduled reports covering alerts and incidents.
     - › User Activity
     - › Configuration Changes
     - › Failed logins
     - › Attacks from specific sources
4. ***Identify the biggest threats***
   - Scammers
   - Hackers (including state-sponsored hackers)
   - Internal bad actors
5. ***Identify your organization's assets and update your response plan***
   - Baseline (today)
   - When you add systems
   - When you remove systems
6. ***Ensure your cybersecurity plan grows and changes as your organization does***
   - Periodically test your plan with tabletop exercises and live simulations
   - Ensure your backup and disaster recovery plan accounts for cybersecurity attacks
   - Consider implementing multi-factor authentication
7. ***Don't forget physical security:***
   - Keep passwords secure
   - Control access to networking devices

About Us

Scantron Technology Solutions provides managed print and IT services you can count on. Our nationwide team of experts provide full-service packages and á la carte options to be your IT team or to support your current staff. Scantron solutions meet you where you are and help you get to where you want to be.