February | 2026

SAFETY NET

NJSIG'S SAFETY NEWSLETTER

Social Engineering on the Rise in K-12 Schools

Social engineering: *A type of cyberattack that relies on psychological manipulation rather than technical hacking to trick people into revealing sensitive information, clicking harmful links, or granting unauthorized access to systems.*

Cybercriminals increasingly target K–12 schools by impersonating trusted administrators, vendors, or colleagues using realistic emails, calls, or messages. Powered by AI, these attacks are more frequent and convincing than ever, leaving schools especially vulnerable to data breaches, ransomware, and financial loss.

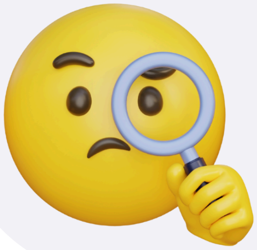
Read More...

Tips from NJSIG Cyber Experts

When in doubt, double check!

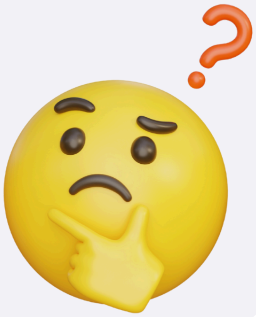
Members should always double-check any request to change a payment method using a trusted channel, not just email. ***A quick phone call to verify can go a long way in stopping a potential malicious attack!***

Tony Fernandez
NJSIG E&O Claims Supervisor



What to do:

- **Always** have a trusted contact at the vendor and confirm any changes (especially payment-related ones) through a channel ***other*** than email.
- **Never** take email change requests at face-value. **Always** double check.



Be vigilant & suspicious!

*Take **a moment to pause** and ask yourself if an email, text, or phone call really seems legit. Be on the **lookout for red flags** like typos, urgent "act now" messages, requests for sensitive info, sketchy links, or email addresses that feel just a little off.*

Jeff Cook

NJSIG IT Manager

What to do:

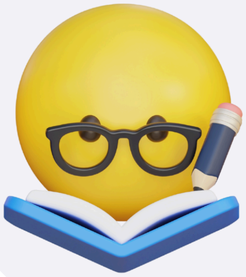
- If a message sems suspicious, **it likely is suspicious**.
- Attackers count on you reacting fast without thinking. If something feels rushed or high-pressure, **slow** the interaction down and **take a closer look**.

Training matters!

*Don't treat training as something you do just to satisfy a policy requirement**; it's a vital necessity.** As cyber threats grow more complex and evasive, quality training becomes **our first line of defense.***

Ricky Caraballo

NJSIG IT Security Specialist



What to do:

- Attackers exploit human psychology (things like trust, fear, and curiosity) to get around technical safeguards such as **firewalls**.
- Regular training **helps reduce** the chances of a successful breach, protecting against costly downtime, data theft, and damage to your school's reputation.

Vector Solutions Cyber Training

Vector Solutions™

NJSIG offers members free access to the Safety & Compliance Library via the Vector Training System (formerly SafeSchools). Trusted by K-12 administrators, it provides expert-led online courses on safety, prevention, and inclusive instruction—convenient, high-quality training that saves time and resources. The following cybersecurity courses are available to our members at no cost, under the **Information Technology Library.**

Training Name	Duration
Cybersecurity Overview	15 minutes
Email and Messaging Safety	23 minutes
Online Safety: Predators	19 minutes
Online Safety: Threats of Violence	16 minutes

Online Safety: What Every Educator Needs to Know	19 minutes
Password Security Basics	10 minutes
Protection Against Malware	17 minutes

For Vector Solutions support, contact their Customer Care Team at 1-866-202-9455 Ext. 3, or visit the **Support Center**.

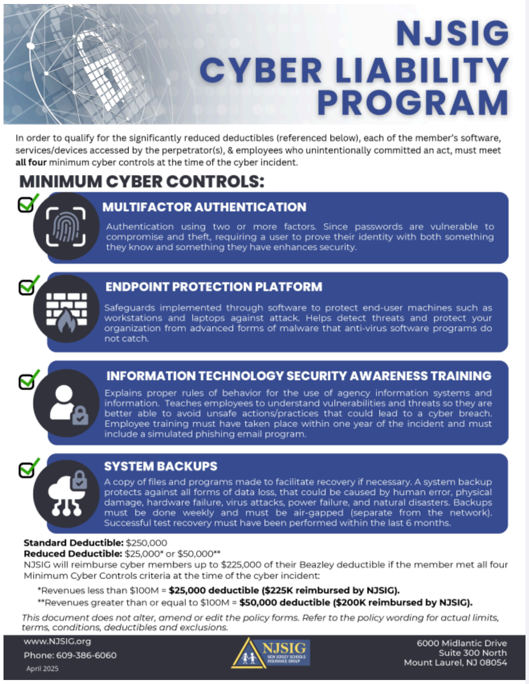
NJSIG Cyber Liability Program

NJSIG, in partnership with **Beazley Insurance Company**, reminds members of the **four minimum cybersecurity controls** that should already be in place. These measures help protect schools from cyber threats while also lowering cyber deductibles and supporting a more sustainable cyber program over time.

Minimum cyber controls:

1. Multifactor authentication;
2. Endpoint protection platform;
3. Information technology security awareness and training program; and,
4. System backups.

To qualify for the reduced deductible, the member must meet ***all four*** *minimum cyber controls listed above at the time of the incident. That means: (1) each of the member's software, services, or devices accessed by the perpetrator(s) must have been protected by at least one (1) layer of multifactor authentication; (2) each device accessed by the perpetrator(s) must have been safeguarded by endpoint protection software; (3) employee(s) who unintentionally committed an act must have had information technology security awareness training (which they must have included a simulated phishing email program) within one (1) year of the incident; and (4) the member's systems must have been protected through an air-gapped backup with a test recovery having been successfully performed within six (6) months of the incident.*



NJSIG
CYBER LIABILITY
PROGRAM

In order to qualify for the significantly reduced deductibles (referenced below), each of the member's software, services/devices accessed by the perpetrator(s), & employees who unintentionally committed an act, must meet **all four** minimum cyber controls at the time of the cyber incident.

MINIMUM CYBER CONTROLS:

☑ MULTIFACTOR AUTHENTICATION

Authentication using two or more factors. Since passwords are vulnerable to compromise and theft, requiring a user to prove their identity with both something they know and something they have enhances security.

☑ ENDPOINT PROTECTION PLATFORM

Safeguards implemented through software to protect end-user machines such as workstations and laptops against attack. Helps detect threats and protect your organization from advanced forms of malware that anti-virus software programs do not catch.

☑ INFORMATION TECHNOLOGY SECURITY AWARENESS TRAINING

Explains proper rules of behavior for the use of agency information systems and information. Teaches employees to understand vulnerabilities and threats so they are better able to avoid unsafe actions/practices that could lead to a cyber breach. Employee training must have taken place within one year of the incident and must include a simulated phishing email program.

☑ SYSTEM BACKUPS

A copy of files and programs made to facilitate recovery if necessary. A system backup protects against all forms of data loss, that could be caused by human error, physical damage, hardware failure, virus attacks, power failure, and natural disasters. Backups must be done weekly and must be air-gapped (separate from the network). Successful test recovery must have been performed within the last 6 months.

Standard Deductible: $250,000
Reduced Deductible: $25,000* or $50,000**
NJSIG will reimburse cyber members up to $225,000 of their Beazley deductible if the member met all four Minimum Cyber Controls criteria at the time of the cyber incident:

*Revenues less than $100M = **$25,000 deductible ($225K reimbursed by NJSIG).**
Revenues greater than or equal to $100M = **$50,000 deductible ($200K reimbursed by NJSIG).

This document does not alter, amend or edit the policy forms. Refer to the policy wording for actual limits, terms, conditions, deductibles and exclusions.

www.NJSIG.org
Phone: 609-386-6060
April 2025

NJSIG
NEW JERSEY SCHOOLS INSURANCE GROUP

6000 Midlantic Drive
Suite 300 North
Mount Laurel, NJ 08054

Download NJSIG's Cyber Liability Guide

Reporting a Cyber Incident

For those covered by **NJSIG's cyber liability insurance**, it is essential to follow the correct protocol for reporting incidents.

Any cyber or privacy incidents should be reported directly to Beazley Breach Response via email at **bbr.claims@beazley.com**. While

the 24-hour hotline (866-567-8570) is also available, **email is strongly recommended for a faster response.**

After reporting to Beazley, a notification of the filing should also be sent to NJSIG at **froi@njsig.org**.

Stay informed with NJSIG!
Have a colleague stay in the know, too!
Sign up here

SafetyNet Newsletter Archives

New Jersey Schools Insurance Group | www.njsig.org