October 2024

NEWS @ NJSIG

NJSIG
NEW JERSEY SCHOOLS INSURANCE GROUP

Phishing Alert: How Vigilance and Quick Action Prevented a Costly Scam

As cyberattacks and data breaches become more frequent, it is crucial for everyone to understand phishing and to consistently verify the legitimacy of emails, and what better time to discuss those topics than during **Cybersecurity Awareness Month**!

We don't need to look very far to understand why vigilance is so important, as we recently foiled what could have been a disastrous six-figure phishing attack involving a member's compromised email account and NJSIG's Accounting Department. The attacker apparently gained access to the member's email and monitored the communications between the school district and NJSIG. The would-be thief then created a fake email domain which replaced the lowercase "i" in "@njsig.org" with a lowercase "L," and inserted themselves into the email chain in the hopes that the member wouldn't notice the subtle difference. Posing as an employee from NJSIG's Accounting Department, the threat actor tried to trick the member into setting up an electronic money transfer which, if completed, would have cost the member over $400,000. Fortunately, the member found the request to be suspicious and contacted NJSIG directly for clarification. Thanks to the member's attentiveness, NJSIG quickly identified the incident as a phishing attempt and prevented the loss from occurring.

On the Lookout

NJSIG wants to remind members that if a message looks suspicious, it could be a phishing attempt. According to **cyber.nj.gov**, be on the look-out for these tell-tale signs of phishing:

- **Does the email ask for sensitive information?**
- **Is the sender address and domain legitimate?**
- **Does this email contain links that do not match the sending domain?**
- **Is the email personalized?**
- **Is there poor spelling or grammar in this email?**
- **Are there phrases or tactics often used to convince recipients into opening links or attachments?**

Click here for more information on how to avoid phishing scams.

Secure Your Banking

In an attempt to safeguard your assets, NJSIG recommends that each member contact their banking institution to confirm (or set up) all banking accounts have bank recommended security safeguards in place.

Implement Cybersecurity Controls

Further, since the education/research sector has historically faced the greatest number of cyterattacks, **NJSIG** would like to remind members of the four **minimum cybersecurity controls** they must implement in order to be eligible for a reduced cyber claim deductible. These security measures are designed to help keep schools safe from cyberattacks and, in turn, make for a more sustainable cyber program in the long term.

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.*

**The above summary is for informational purposes only and is not intended to amend, modify, supplement, or alter any insurance policy. Eligibility for the reduced cyber premium will be determined in accordance with the actual terms and conditions of the applicable NJSIG cyber policy, which readers are encouraged to review carefully to ensure compliance.*

Click here to download NJSIG's cyber liability flyer

Click here for additional cybersecurity resources

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.
