CYBER INSIGHTS

LloydSadd

NAVACORD®

4 Reasons Why Cybersecurity Training Fails

Allianz's 2023 risk barometer reported that cyber incidents topped the list of risks facing businesses worldwide in 2023 for the second year in a row, making thorough staff training and a strong cybersecurity culture more important than ever.

Indeed, cybercriminals continue to adapt their tactics to exploit victims, and new technologies like ChatGPT could make cyberattacks harder to spot. Therefore, cybersecurity awareness training must include the latest information. Unfortunately, such training programs aren't always successful, and knowing why can help you avoid similar pitfalls.

Consider the following four reasons why cybersecurity fails:

1. **Training gives limited context.** Many training programs include general cybersecurity guidance rather than industry-specific information. For instance, generic phishing emails (e.g., a fraudulent Netflix account reset email sent to a business address) often form the bulk of training examples, which can disengage employees who don't see the relevance. Instead, include specific training examples, give context to why training sessions are important and explain how teachings fit into broader cybersecurity goals.
2. **Training includes few topics.** Programs often focus too much on phishing. While phishing is a significant threat to businesses and deserves considerable attention, other cyberattack tactics are on the rise. Ensure training incorporates a range of topics, including current trends and regulatory requirements.
3. **Training blames the victim.** Sometimes, training puts the victim at fault for clicking suspicious links or falling for scams. Such notions could make employees less likely to report suspicious behaviour for fear of being criticized. Thus, make sure training supports employees and empowers them to take action.
4. **Training excludes managers.** Training programs may focus on the general workforce and exclude board members or senior leadership. This strategy creates the impression that management is not invested in cybersecurity nor values its importance. Instead, create a culture where cybersecurity is everyone's responsibility.

If you have questions specific to your business, or would like additional information, please reach out to your Lloyd Sadd Advisor.

LET US HELP YOU MANAGE YOUR RISK

Edmonton: 1.800.665.5243
Calgary: 1.866.845.8330
Kelowna: 1.800.665.5243

lloydsadd.com
info@lloydsadd.com