



Data Breach Fatigue – The Danger of Becoming Complacent

One might think the logical response to hearing about the vast number of breaches in the news would result in a more proactive mentality within corporate America. However, data breach fatigue is just what it sounds like – the misperception that hacking events and identity loss are just unavoidable realities of everyday life.

“With this data breach fatigue attitude, organizations really put themselves at risk,” says Chris Christians, Business Development Manager at LifeLock. “Of the companies I’ve worked with this year looking for a breach solution, a vast majority of them have under 1,000 employees. Many were breached by a low-tech but very potent W2 phishing scam, where only one employee made the mistake of passing along vital personnel information. So unfortunately, even if companies invest in various technologies or infrastructure to manage security, the hackers will typically find an end-around.”

“What I recommend is that companies invest in their employees, not just in their security technology. I work in the breach business where we hear the all-to-common stories of companies having no action plan for when a breach hits. We have CEOs and lawyers reaching out to us after a breach has occurred asking for advice.”

“For these small to medium sized businesses, it’s a far better investment in time and money to be proactive and have an identity theft protection solution in place before something happens. The hackers and their schemes are not going away anytime soon, so again it’s not about waving a white flag surrendering to fate, it’s about being proactive and protecting your people.”

“From our experience, especially this year, smaller non-Fortune 500 companies face even more risk.

They are typically not as prepared and less educated on preventative measures. Also, lower-tech phishing scams, like the W2 one, have typically been more successful because employees are more prone to passing information along because they know most of the people in their company and are not as suspicious of the request.”



**LEARN MORE ABOUT THE
WORLD’S BIGGEST DATA BREACHES**