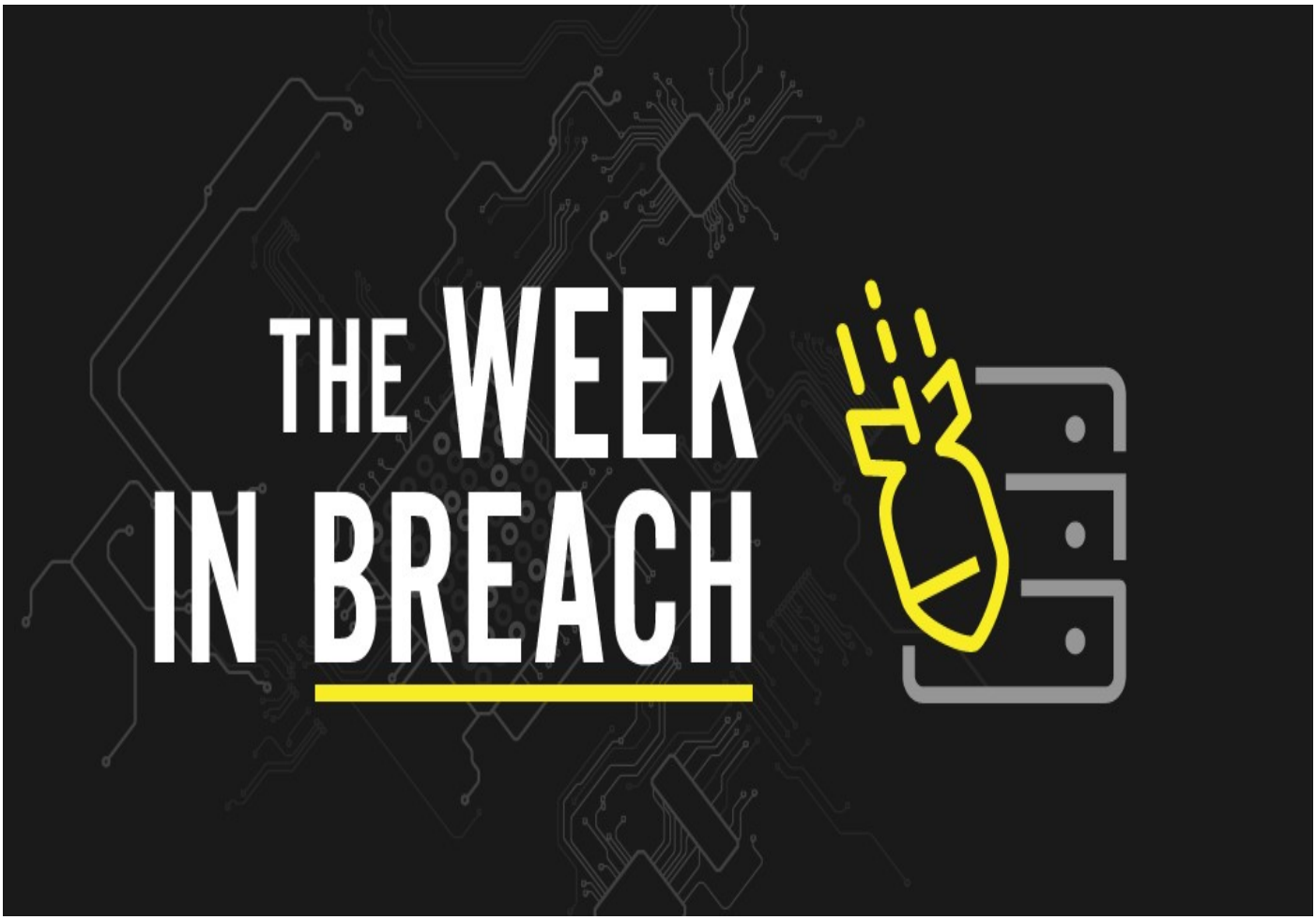
THE WEEK IN BREACH NEWS: 11/02/22 - 11/09/22

DenBe Computer Consulting
Connecting Business

November 9th, 2022 by Dennis Jock



If your business isn't using our ***Dark Web Monitoring Services*** please call us for a free scan and to discuss setting up this cutting edge monitoring service for you!

Not ready to talk yet? Visit our website to get your ***FREE Dark Web Scan.*** You will get a free, no obligation scan sent to your inbox within 24hrs. ***Visit today: www.denbeconsulting.com***

Bed, Bath and Beyond
https://www.reuters.com/business/retail-consumer/bed-bath-beyond-reviewing-possible-data-breach-2022-10-28/?utm_campaign=fullarticle&utm_medium=referral&utm_source=inshorts

Exploit: Phishing

Bed Bath and Beyond: Home Goods Retailer

Risk to Business: 1.863 = Severe

Big-box retailer Bed, Bath and Beyond has experienced a data breach. The company disclosed that a third party had improperly accessed its data through a phishing scam. Bad actors gained access to the hard drive and certain shared drives of one of its employees earlier this month. The retailer was quick to reassure consumers that it does not believe that any sensitive or personally identifiable information was accessed.

How It Could Affect Your Business: Phishing takes down businesses of every size and every industry, bringing sticky problems in its wake.

See Tickets US
https://www.bleepingcomputer.com/news/security/see-tickets-discloses-25-years-long-credit-card-theft-breach/

Exploit: Hacking

See Tickets US: Event Ticketing Platform

Risk to Business: 1.423 = Extreme

The U.S. division of UK company See Tickets has revealed that its platform has been hosting a credit card skimmer for an estimated two and a half years. In a data breach notification shared with the Montana Attorney General's office, See Tickets disclosed that it discovered the breach in April 2021 and ultimately determined that the skimmer was activated on June 25, 2019. However, it wasn't until January 8, 2022, that the malicious code was fully removed from its site. The company says that it worked with forensic experts and Visa, MasterCard, American Express and Discover in the investigation.

Individual Risk: 1.307 = Extreme

The customer information that the hackers might have stolen includes a client's full name, physical address, ZIP code, payment card number, card expiration date and CVV number. No number of clients affected was specified.

How it Could Affect Your Business: This is going to be an expensive, damaging nightmare thanks to it going on for so long, putting the company's security commitment in question.

Kenosha Unified School District
https://www.scmagazine.com/brief/ransomware/wisconsin-school-district-attacked-by-snatch-ransomware-group

Exploit: Ransomware

Kenosha Unified School District: Local Education Authority

Risk to Business: 2.687 = Moderate

Kenosha Unified School District in Wisconsin has been the victim of a successful ransomware attack by the Snatch ransomware group. The gang added the district to its dark web leak site last week. Kenosha Unified School District officials admitted that the district was forced to take systems offline to deal with the attack but they've since been restored. No ransom amount has been reported, nor did the district elaborate on what data had been stolen. The district serves an estimated 20,000 students.

How It Could Affect Your Customers' Business: Schools at every level and education authorities have been getting pounded by ransomware groups and need to improve their defenses.