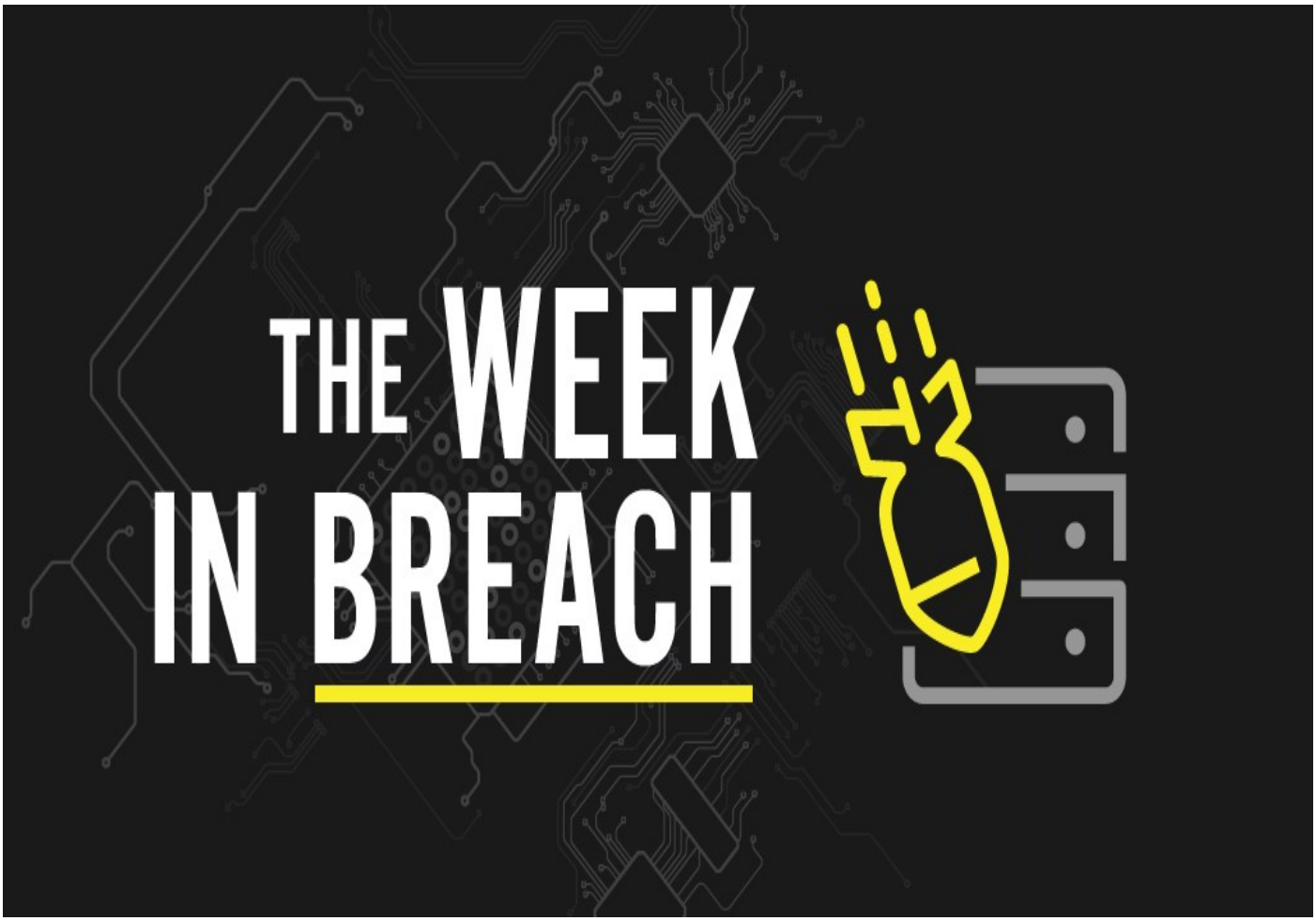
THE WEEK IN BREACH NEWS: 09/20/22-09/27/22

DenBe Computer Consulting
Connecting Business

September 28th 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***

U.S. Internal Revenue Service (IRS)

https://news.yahoo.com/irs-inadvertently-publishes-120-000-234841222.html

Exploit: Human Error

U.S. Internal Revenue Service: Federal Government Agency

Risk to Business: 2.026 = Severe

The U.S. Internal Revenue Service on Friday acknowledged that thanks to an employee error, the agency accidentally published confidential information about 120,000 taxpayers on its website. The compromised data came from Form 990-T filings. This form is required for people with individual retirement accounts who earn certain types of business income within retirement plans. While the forms for individuals are supposed to be confidential, charities that generate certain types of income are also required to file Form 990-T, and those are intended to be public. An employee mistakenly uploaded private taxpayers' data to the agency's website along with the public charity data.

Risk to Individual: 2.406 = Severe

Exposed taxpayer data includes names, contact information, and financial information about IRA income The exposed data did not include Social Security numbers, full individual income information, detailed financial account data, or other information that could impact a taxpayer's credit.

How it Could Affect Your Business: Human error is the top cause of cybersecurity trouble, but training helps reduce the risk of a data disaster related to employee mistakes.

U-Haul International
https://www.bleepingcomputer.com/news/security/u-haul-discloses-data-breach-exposing-customer-driver-licenses/

Exploit: Credential Compromise

U-Haul International: Moving & Storage Company

Risk to Business: 2.779 = Moderate

U-Haul International disclosed a data breach related to its customer contract search tool. U-Haul says that attackers accessed some customers' rental contracts between November 5, 2021, and April 5, 2022, after compromising two passwords. U-Haul's email and customer-facing websites were not impacted.

Risk to Individual: 2.626 = Moderate

Hackers gained access to customers' names and driver's license information, but U-Haul says that no credit card information was accessed or acquired during the incident.

How it Could Affect Your Business: Cybercriminals have been concentrating their fire on suppliers and service providers, elevating risk for them.

The North Face
https://www.bleepingcomputer.com/news/security/200-000-north-face-accounts-hacked-in-credential-stuffing-attack/

Exploit: Credential Stuffing

The North Face: Clothing Brand

Risk to Business: 1.677 = Severe

California-based outdoor clothing company The North Face disclosed that it has had a data breach after a successful credential stuffing attack exposed the information of an estimated 200,00 customers. The company said that the attack on its website began in late July 2022 and was finally stopped in August 2022. Investigators determined that bad actors had accessed shoppers' information shortly thereafter.

Risk to Individual: 1.636 = Severe

Exposed data includes a customer's full name, purchase history, billing address, shipping address, telephone number, account creation date, gender and XPLR Pass reward records.

How it Could Affect Your Business: Educational institutions have been high on cybercriminal priority lists, and the time pressure here made this attack an attractive prospect for the bad guys.