Phishing in Troubled Waters

Control.My.ID

Small Business Security & Privacy
Case Study Series

Business as Usual

The business that was targeted is a business that has no retail locations and provided consultancy to other businesses. They used their website to capture new leads, interact with customers, and provide various online services.

Dark Web of Knowledge

The business was notified that they had data being sold on a dark web marketplace that was being marketed as belonging to them. The data was checked by the business and verified to belong to them but was "very outdated." However, the business was able to identify that the breached password was reused elsewhere that put other services and money at risk.

Cause & Effect

The cause of the data leak was tracked back to a phishing email, masquerading as an HR-related topic for a particular employee by the payroll processor. It is believed the bad actor knew employee names and was trusted by an HR employee because it appeared the email not only had the employee name but seemed to originate from the payroll processor used by the business. Notifications of the data breach had to be sent out to employees and customers, causing a loss in trust as well as some cancellations of existing customers, totaling in excess of $50,000 in annual revenue. The business found that an additional $200,000+ was at risk due to the reused password and was able to change the password before it was accessed by a bad actor.

An Ounce of Prevention

The business trains their employees to be on the lookout for phishing emails. However, human error is always a possibility. This business uses the Control.My.ID Small Business Security & Privacy Tool to monitor breaches to catch breached data that puts them at risk.