Opinion

What happens in breach, how to respond

CYBER SECURITY

KELLY BOURNE

It's impossible to know exactly how many passwords are in use worldwide, but in 2017, Inc. magazine predicted there would be 300 billion of them by 2020. That worked out to be about 38 passwords per resident of planet Earth. It isn't important whether that estimate was high, low or exactly right. The most critical question is whether the organizations that hold them are storing them securely or not.

Unfortunately, not all these billions of passwords are safe.

Data breaches are security incidents where confidential information is exposed to unauthorized parties. The types of data exposed includes logon credentials (account IDs and passwords), Social Security numbers, bank account numbers, street addresses, e-mail addresses and driver's license numbers.

In 2024 almost 2 billion people were known to have had their personal data exposed in data breaches.

Some of the largest data breaches in 2024 were:

■ **National Public Data** lost 2.9 billion records including personally identifiable information, addresses and Social Security Numbers in 2023 and 2024.

■ **AT&T** phone records of almost all its customers were stolen by hackers in April 2024.

■ **United Healthcare** lost records including protected health information belonging to more than 100 million people in 2024.

■ **Ticketmaster** lost data belonging to more than 500 million individuals in a 2024 breach. The data exposed included names, addresses, e-mail addresses and credit card details.

Some of the more common causes of data breaches are:

■ **Insider threats** — When employees of an organization steals and sells information from their employer.

■ **Social engineering** — Attacks used to trick someone at the targeted organization into revealing sensitive information, like their account ID and password. Once the bad actor has that information, it can be used to access databases with personal information of clients, customers, employees, etc.

■ **Viruses or other malware** — These can be used to attack an organization's systems. Viruses can be installed on a target computer if an employee at the organization opens an infected e-mail attachment or clicks on an e-mail link that leads to an infected website. Once the virus executes, it can give the attacker access to the organization's computers or network.

■ **Lost or stolen passwords** — These can lead to unauthorized access and potentially a data breach at an organization.

■ **Software errors** — If an organization doesn't apply patches and upgrades from the vendors, then an intruder can take advantage of vulnerabilities to access the firm's computers and potentially cause a data breach.

Once a criminal has stolen personal information from an organization, he will try to use it himself or make money from it. Common ways to exploit stolen data are:

1. Selling it on the dark web — Estimates of what personal information is sold for on the dark web range widely, but some examples are: credit card details are worth between $10 and $100. Online bank account information can sell for $100. Facebook account credentials are worth $45. PayPal account logins can sell for $150.

2. Retaliation — In some instances, a bad actor may post credentials and other personally identifiable information on the internet where anyone can access them for free. This might be done to punish the organization from which the data was stolen

3. Credential stuffing attacks — Stolen account credentials can be used in a credential stuffing attack. In this type of attack a list of stolen credentials will be used to try to log into many websites. Examples of websites are Facebook, PayPal, Netflix, Amazon, e-mail providers or major banks. If a person used the same password for multiple websites, this type of attack can allow the hacker to take over numerous accounts.

Members of the public might ask how they can tell if their data was exposed in a data breach. Some answers to that important question are:

■ When an organization learns that their system has been breached and there is a reasonable chance that personal information has been exposed, they may be required by state and federal laws to send out data breach notifications to all affected individuals. Getting a breach notification via e-mail or a letter is one way consumers learn about the breach.

■ Cybersecurity companies monitor the dark web where confidential data is frequently bought and sold. If data belonging to one of their clients is identified they will alert that client.

■ Consumers can use websites like www.haveibeenpwned.com, www.f-secure.com, www.keepersecurity.com and uk.norton.com to see if their e-mail addresses or passwords have been exposed on the dark web.

If you learn that your data has been breached some steps that you should perform include:

■ Take advantage of free credit report monitoring that the affected organization is likely to offer.

■ Consider placing a credit freeze or fraud alert with the major credit bureaus.

■ Change the password and if possible, the username (account ID) of affected accounts.

■ If you can't log into one of your accounts, then it is possible that it has been taken over by a cybercriminal. Contact the organization and request assistance to regain control of the account.

■ If you used the same password for other accounts change the passwords on those sites too.

Consumers can't prevent their data from being exposed by data breaches. Protecting our personally identifiable information is the responsibility of the banks, retailers, government agencies, hotels, data brokers, casinos, credit bureaus, schools, etc. that are using and storing it. But there are steps consumers can take to reduce the odds or minimize the damage if their credentials are exposed by a data breach.

■ Use multi-factor authentication for your online accounts. If a criminal learns your password, then MFA will prevent him from accessing the account.

■ Don't use the same password for multiple online accounts.

■ If the website allows it, set it so multiple failed login attempts will lock the account temporarily, e.g. for 30 minutes or an hour.

■ Change your passwords periodically.

■ If you learn that a vendor or website you have an account with has been hacked then change your password immediately.

■ If you receive a breach notification from a website change that password as well as any other accounts that use the same password.

When we go online, we cede control over our personal data to others and trust that they will safeguard it. Unfortunately, they aren't always worthy of that trust. Hopefully, the information in this article helped you to understand what can happen if sensitive information is breached and how to respond.

Kelly Bourne is the author of "Ransomware, Viruses, Social Engineering and Other Threats: Protecting Your Digital Assets." He lives in Omaha, NE, and may be reached at kcbourne@cox.net.

Law & Order

Man charged for OWI after running stop sign

A 42-year-old Sibley man was arrested about 1:45 a.m. Sunday, Aug. 17, on charges of first-offense operating while under the influence and failure to obey a traffic control device.

The arrest of Gerardo Diaz Gallaga stemmed from the stop of a 2016 Chevrolet Trax on Fifth Street near 11th Avenue in Sibley after he failed to stop for a stop sign, according to the Osceola County Sheriff's Office.

Diaz Gallaga also was slow to pull over for the patrol vehicle's emergency lights but did so after the siren was activated. He had bloodshot/watery eyes, impaired balance and the odor of an alcoholic beverage and failed field sobriety tests. Diaz Gallaga admitted to drinking to beers.

Sibley man cited for no contact violation

A 27-year-old Sibley man was cited Thursday, Aug. 21, for violation of no contact/protective order.

The citing of Saul Vilchis Manon stemmed from him being observed in a food truck with an individual he is not to have contact with at about 5:45 p.m. Thursday, Aug. 21, in Sibley, according to the Osceola County Sheriff's Office.

Kwik Star clerk cited for stealing drinking booze

A 50-year-old Sibley man was cited Thursday, Aug. 21, on a charge of fifth-degree theft.

The citing of Allen Gordon Rolfes stemmed from Kwik Star reporting he stole 50-milliliter liquor bottles while working as an employee and consumed them Aug. 2-5, according to the Osceola County Sheriff's Office.

Kwik Star documented at least 15 bottles were taken along with some almonds for a total of $42.14.

Fifth-degree theft charges involve incidents in which the value of the stolen property is estimated at less than $300.

Briefly

Power Hour program offered through ORHC

Power Hour at Osceola Regional Health Center in Sibley is a circuit-style training that focuses on strength, endurance, power and conditioning in a fun, upbeat atmosphere.

The functional training the class offers is designed with accelerating levels, inclusive to all fitness levels. The goal is to help participants do normal live things easier, stronger and better.

Check out the full class schedule at www.osceolarhc.org/wellness.

Virtual aging caregiver support meetings set

Elderbridge Agency on Aging hosts a Virtual Caregiver Support Group Zoom meeting 10-11 a.m. on the third Tuesday of each month. Learn about the ways Elderbridge can help.

Call Ally Schwartzkopf for the Zoom link at 1-800-243-0678.

Ministry available to address range of issues

The Osceola County Ministerial Association is providing a Christ-centered recovery program for life's hurts, habits and hang-ups.

The ministry can serve a variety of issues from habitual sin, loneliness, codependency, addiction or whatever hurt, habit, or hang-up participants want to work on. The program is open to adults 18 and over. A typical Monday night will have worship, teaching, fellowship and small groups. Doors open at 6:15 p.m. at Sibley Christian Reformed Church, 115 Maple Drive.

For more information, contact Pastor Ben Wiersma at 712-461-1400.

Grants, loans available for projects for homes

The Northwest Iowa Regional Housing Trust Fund provides financial assistance to low- to moderate-income homeowners for necessary repairs to their homes. Financial aid will be available in grants and low-interest loans. Applications may be picked up at any city office or by calling Kristin Larsen at 712-262-7225 Ext. 139.

Gazette-Tribune THE OSCEOLA COUNTY
ESTABLISHED IN 1872

ADDRESS: P.O. Box 160, Sheldon, IA 51201 **PHONE:** 712-324-5347 **FAX:** 712-324-2345

CIRCULATION: The Osceola County Gazette-Tribune is an official legal newspaper for Sibley and Osceola County and is published weekly on Wednesdays.

PERIODICALS POSTAGE: The Osceola County Gazette-Tribune is entered and periodicals postage paid at Sibley, IA 51249
USPS 611-120

SUBSCRIPTIONS: All copies sent through the U.S. Postal Service at a rate of $45.00 for one year, in advance, in Clay, Lyon, O'Brien, Osceola, Sioux, Dickinson and Plymouth Counties, and 57.00 per year everywhere else. Single copies can be purchased for $1.50.

CIRCULATION: circ@iowainformation.com
BILLING: accounting@iowainformation.com
NEWS: gtnews@nwestiowa.com
ADVERTISING: ads@iowainformation.com
LEGALS: legals@iowainformation.com

POSTMASTER: Send address changes to The Osceola County Gazette-Tribune, P.O. Box 160, Sheldon, IA 51201. You also may submit your address change online at www.nwestiowa.com/submit and select "Change of address."

PUBLISHER: Peter W. Wagner
EDITOR: Jeff Grant
PRESIDENT: Jeff Wagner