THE Wealth REPORT

IMPLICATIONS OF HAVING YOUR DATA EXPOSED

Overview

To pull off the most valuable score, thieves once had to physically break into a brick-and-mortar building, and once inside, force open a locked safe. Back then, cash was criminals' hottest commodity because it could be spent without having to find a buyer.

These days, consumer data is the most valuable stolen good. Cyberthieves can remotely "break in" to a company's computer system from the comfort of their own home. They also have a ready market of buyers willing to pay for volumes of private information. It's as easy as 1-2-3:[2]

1. Research. A cybercriminal scans the network security of various companies looking for a vulnerability that can be infiltrated.
2. Attack. There are two ways a cyberthief can gain access:
   a. Network attack: The hacker uses infrastructure, system and application weaknesses to infiltrate an organization's network.
   b. Social attack: The hacker tricks or baits employees into opening an email, clicking a link or an attachment that provides access to the company's network, often by hacking the employee's own computer for login credentials.
3. Exfiltration. Once the hacker has access to a company network, private customer data and/or proprietary company information is extracted.

In 2018, Bloomingdale's, Macy's and Reddit were added to a growing list of companies infiltrated by data hackers.[1] While a security breach can become a public relations nightmare for the affected company, the real damage is inflicted on the consumers whose data was left unprotected.

10 Largest Data Breaches[3]

(as of December 2018)

Company/Organization	Records Stolen	Date
Yahoo	3 billion	08/13
Marriott International Inc[4]	383 million	11/18
Equifax	145.5 million	07/17
eBay	145 million	05/14
Heartland Payment Systems	134 million	03/08
Target	110 million	12/13
TJX Companies (TJ Maxx, Marshalls)	94 million	12/06
JP Morgan & Chase	83 million	07/14
Uber	57 million	11/17
U.S. Office of Personnel Management	22 million	2012-2014
Timehop	21 million	07/18

Type of Information Stolen

Targets vary based on the type of information hackers seek. In addition to customer data from businesses, breaches have occurred at medical/health care companies, government and military installations, banking/credit/financial organizations and educational institutions.

It's remarkable how many different types of personal information that, in the hands of a fraudster, can be damaging to any one person — particularly with regard to finances. Even more concerning is the fact consumers have so freely provided this information to hundreds of companies and institutions while trusting the private data will be kept secure and confidential.

Here's a sample of the most potentially damaging information consumers routinely give out or store on computers and cellphones:[5]

- Full legal name
- Mailing and/or physical address
- Telephone number
- Email address
- Date of birth
- Social Security number
- Driver's license number
- Member identification numbers
- Financial account numbers
- Insurance policy numbers
- Personal medical information
- Website passwords
- Passport number
- Personal photos and videos

Cyberthieves can use this data to duplicate credit cards, steal a person's identity, make fraudulent charges, siphon money from accounts and even blackmail victims. Computer hackers don't even need to commit subsequent frauds. They can sell consumer data individually or in bulk on the Dark Web, explained below.

What Happens To Stolen Data

To fully appreciate what can happen to stolen data, it's important to understand the three basic layers of the internet.[6]

1. Surface Web — This is all of the accessible data we can reach by search engines such as Google and Bing. Plug in a search for your home address, and you may get a Google Map of its location and various real estate websites that provide a market value of your home. However, you won't find information about how much you paid in property taxes on your home last year.

2. Deep Web — This is information that is not organized, catalogued and searchable by a search engine. However, we can uncover it by visiting specific websites. Visit your local tax appraiser's website, and you may be able to conduct a search for your property to find out how much you paid in property taxes.

3. Dark Web — This is the hidden part of the internet that is not accessible by conventional means. People who use the Dark Web must download a different type of software to access websites with the .onion extension. Located on this layer of the web are specific marketplaces that buy unlawfully obtained information as well as other illicit goods and services. The Dark Web also provides communication vehicles for people who require complete secure and untraceable means, such as journalists and whistleblowers and citizens who live in oppressive regimes.

The Dark Web features a wide range of black-market websites and discussion forums, where stolen data is packaged, processed and sold in volume quantities — usually paid for in untraceable currencies such as bitcoin. One security firm estimates more than 24 billion credentials have been shared over the Dark Web.

The following are statistics that give you an idea of how stolen data is sold and used:[7]

- Hackers pair stolen data with personal photos to create fake IDs.
- A comprehensive file for one individual — called a "fullz" — may include a victim's date of birth, Social Security number, telephone number, driver's license number and banking information. One fullz sells for about $100.
- Data that offers access to at least $15,000 in a bank account sells for about $1,000.
- SIM hijacking is when a criminal uses stolen data to convince a cellphone carrier they lost their phone and need a new SIM card. The new SIM card provides access to the victim's phone number, which can be used to reset online passwords and drain financial accounts.
- Login information for specific company email addresses sells for $400 to $500.

International Laws

Plenty of countries passed laws instructing how companies are to use and protect consumer data. The European Union, for example, enforces rules under the General Data Protection Regulation. Companies are required to communicate all the ways they plan to use collected data and must actively seek consent from customers to do so. The regulation also enables customers to formally request removal of their data, and organizations are required to inform users of any security breach within three days, with substantial fines for noncompliance.

The United States has yet to pass laws detailing how user data must be handled. There is a quagmire of industry-specific rules and regulations, such as those that apply to medical data, financial data or data related to minors. While some rules may limit what data an organization is permitted to gather and how it must be stored and accessed, there is no comprehensive set of rules and ramifications in place.[8]

For example, a website may be required to publish a privacy policy, but even those commonly state the site shares collected consumer data with third parties. The requirement is simply to publish a policy concerning privacy; not that data is kept private.

"So much stolen data is available on the Dark Web, people shouldn't worry whether their information has been swiped. Every American person should assume all of their data is out there." [9]

- Elvis Chan, FBI

Final Thoughts

If you wonder who on earth would actually bother to hack into your specific computer, the number is probably quite low. That's because hackers seldom target one individual. They infiltrate large companies with sophisticated network security because they want to steal volumes of confidential data in one fell swoop.

Unfortunately, given the degree we share information like credit card numbers on a daily basis, it's very likely that each of us will one day have our data breached and sold. Not everyone who has their private data pilfered ends up being impacted, but it still pays to protect yourself.

The following are some tips to help you prevent and/or respond proactively to a breach.[10]

- Contact your bank(s), including credit card issuers, if you've been breached. See if you can set up alerts for charges. Verify your current charges and change PIN codes.
- Don't click on suspicious-looking links or download files from unsolicited sources. This is especially true with a work email.
- If you've been notified of a breach, contact the company and ask them to pay for you to enroll in a fraud victim assistance program.
- Use two-factor authentication whenever it is offered, which typically involves receiving a code via text to input when you log into a website.
- Create complex passwords, and use a password manager app to keep track of them.
- Register for an account with the Internal Revenue Service and Social Security Administration. If you're already registered, it's more difficult for someone else to try to do so in your name.
- Look into using a free credit freeze that you can turn on and off as necessary.

[1] TrendMicro. Aug. 10, 2018. "Data Breaches 101: How They Happen, What Gets Stolen, and Where It All Goes." https://www.trendmicro.com/vinfo/us/security/news/cyber-attacks/data-breach-101. Accessed Jan. 21, 2019.

[2] Ibid.

[3] Ibid.

[4] Kirsten Grind and Dustin Volz. Marketwatch. Jan. 4, 2019. "Marriott says hackers swiped millions of passport numbers, but fewer than initially feared." https://www.marketwatch.com/story/marriott-says-hackers-swiped-millions-of-passport-numbers-but-fewer-than-initially-feared-2019-01-04. Accessed Jan. 21, 2019.

[5] TrendMicro. Aug. 10, 2018. "Data Breaches 101: How They Happen, What Gets Stolen, and Where It All Goes." https://www.trendmicro.com/vinfo/us/security/news/cyber-attacks/data-breach-101. Accessed Jan. 21, 2019.

[6] Dark Web News. "Deep Web: What Is It and How To Access It." https://darkwebnews.com/deep-web/#chapter1. Accessed Jan. 21, 2019.

[7] Robert McMillan. The Wall Street Journal. Dec. 9, 2018. "Thieves Can Now Nab Your Data in a Few Minutes for a Few Bucks." https://www.wsj.com/articles/what-happens-to-your-data-after-a-hack-1544367600. Accessed Jan. 21, 2019.9. Accessed Jan. 8, 2019.

[8] Justin Ellingwood. DigitalOcean. Sept. 26, 2017. "User Data Collection: Balancing Business Needs and User Privacy." https://www.digitalocean.com/community/tutorials/user-data-collection-balancing-business-needs-and-user-privacy. Accessed Jan. 21, 2019.

[9] Robert McMillan. The Wall Street Journal. Dec. 9, 2018. "Thieves Can Now Nab Your Data in a Few Minutes for a Few Bucks." https://www.wsj.com/articles/what-happens-to-your-data-after-a-hack-1544367600. Accessed Jan. 21, 2019.

[10] TrendMicro. Aug. 10, 2018. "Data Breaches 101: How They Happen, What Gets Stolen, and Where It All Goes." https://www.trendmicro.com/vinfo/us/security/news/cyber-attacks/data-breach-101. Accessed Jan. 21, 2019.

Investment advisory services offered only by duly registered individuals through AE Wealth Management, LLC. The advisory firm providing you this report is an independent financial services firm and is not an affiliate company of AE Wealth Management, LLC. Investing involves risk, including the potential loss of principal. No investment strategy can guarantee a profit or protect against loss in periods of declining values. The information and opinions contained herein provided by third parties have been obtained from sources believed to be reliable, but accuracy and completeness cannot be guaranteed by AE Wealth Management. This information is not intended to be used as the sole basis for financial decisions, nor should it be construed as advice designed to meet the particular needs of an individual's situation. None of the information contained herein shall constitute an offer to sell or solicit any offer to buy a security or insurance product.