Pegasus Protects- September

This month, we are concentrating on data breaches – examining their nature, causes, and preventative measures. This focus is driven by the increasing incidence of data breaches in recent year.

There was a recent data breach at the National Public Data, a company that is responsible for aggregating data to provide background checks. This incident potentially exposed personal identifiable information including social security numbers. The incident is described in further detail here: https://nationalpublicdata.com/Breach.html .

How do data breaches happen?

A data breach can occur through several avenues, often due to vulnerabilities in cybersecurity, infrastructure or human error. Here's a breakdown of how a breach might occur:

1. Phishing Attacks: Cyber criminals might target employees or customers with phishing emails or messages designed to trick them into revealing sensitive information, such as login credentials or personal identification numbers (PINs). Once obtained, these credentials can be used to access account and extract data.
2. Malware and Ransomware: Attackers might deploy malware, including ransomware, to infiltrate the company's systems. This malicious software can be delivered through phishing emails or by exploiting software vulnerabilities. Once inside the system, it can harvest customer data or encrypt it, demanding a ransom for its release.
3. Weak Passwords and Poor Authentication: If customers or employees use weak passwords or if the company's authentication mechanism are inadequate, attackers can easily gain unauthorized access to sensitive systems. This could lead to a breach of customer data.
4. Insider Threats: Employees with access to sensitive data might intentionally or unintentionally expose this information.
5. Vulnerabilities in Software and Systems: Most companies rely on various software systems for their operations. If these systems have unpatched vulnerabilities, attackers can exploit them to gain unauthorized access to databases containing customer information.
6. Third-Party Vendors: Companies often work with third-party vendors for services such as payment processing, IT support, or data storage. If these vendors have weak security practices, attackers might breach the vendor's system and use it as a backdoor to access the customer's data.
7. Physical Theft or Loss: Sensitive data might be stolen through physical means, such as the theft of devices containing customer information. Similarly, the loss of such devices could result in a data breach if they fall into the wrong hands.

8. Unencrypted Data Transmission: If sensitive data is transmitted over networks without proper encryption, it can be intercepted by attackers. This is particularly risky with unsecured communication channels that can expose customer data.
9. Cloud Security Flaws: Many companies use cloud services for storing and processing data. If the cloud infrastructure is not properly secured, attackers might exploit weaknesses to access customer information.

What You Can Do:

Here are some immediate steps you can take to protect yourself:

1. Monitor Your Accounts: Regularly review your bank accounts, credit card statements, and other financial accounts for any unauthorized transactions. If you notice anything unusual, please contact us immediately.
2. Place a Credit Freeze: Consider placing a credit freeze on your file with the three major credit reporting agencies (Equifax, Experian, and TransUnion). This will prevent new credit accounts from being opened in your name without your consent.
3. Review Your Credit Reports: You are entitled to a free credit report from each of the three major credit reporting agencies every 12 months. Review your reports carefully for any signs of identity theft.
4. Report Suspicious Activity: If you suspect that your Social Security number has been misused, report it immediately to the Federal Trade Commission at https://consumer.ftc.gov/articles/what-know-about-credit-freezes-and-fraud-alerts and consider filing a police report.
5. Update Your Account Security: Consider changing your online banking passwords and enabling two-factor authentication for added security.

In every scenario, the result is the unauthorized access, theft, or exposure of sensitive customer data. This can lead to financial loss, identity theft, and significant damage to the company’s reputation. Preventing data breaches require robust security measures, regular system updates, and strong authentication protocols.

If you have any concerns or questions, feel free to contact us at 214-353-3000.

Credit Bureau links:

Equifax

https://www.equifax.com/personal/credit-report-services/credit-freeze/

Phone number: 888-298-0045

Equifax Information Services LLC P.O. Box 105788 Atlanta, GA 30348-5788

Transunion

https://www.transunion.com/credit-freeze

Phone number: 800-916-8800

TransUnion P.O. Box 160 Woodlyn, PA 19094

Experian

https://www.experian.com/freeze/center.html

Phone number: 888-397-3742

Experian Security Freeze P.O. Box 9554 Allen, TX 75013

Resources:

https://nationalpublicdata.com/Breach.html

https://consumer.ftc.gov/articles/what-know-about-credit-freezes-and-fraud-alerts

https://krebsonsecurity.com/2024/08/national-public-data-published-its-own-passwords/

https://www.usatoday.com/story/tech/2024/08/17/social-security-hack-national-public-data-confirms/74843810007/