JANUARY 28, 2018

2018 Was a Year of Breaches — And It Likely Won't Get Better

Billions Were Breached in 2018

Whether we admit it or not, breaches have become an expectation in today's society. So much so, Fox News Channel 16 reported it is one of the three certainties of life, along with death and taxes. Somber note — but honestly rather accurate considering one billion people had their data stolen in 2018.

So how do you know if you've fallen, victim? And how do you protect your data moving forward? We will start with the former.

First, it is the company's responsibility to notify all potentially impacted customers of a data breach. However, it is best for customers to also stay diligent and not rely on these notifications. Therefore, to determine if your information has been compromised, here are a few tips:

- Use free credit reporting tools to check up on current credit scores and recent activity
- Go to haveibeenpwnd.com and enter your email address to determine if it has been compromised

To be fair, if your personal data was stolen, but has not yet been used maliciously, neither of these two tips will help. This is why we recommend all of our users enroll in an identity theft protection program, like IDShield. Programs such as these will notify a user once their data is used in a questionable manner – like a new line of credit, change of address, new medical information, etc.

Other means of protecting your data include:

- **Stop disclosing everything online** – Blunt but true. Thanks to social media almost anyone can find out where you work, how long you've worked there, your marital status, birth date, anniversary date, children's names, where you grew up, what high school you graduated from, your pet's name — I could really go on and on. My point is, many people use the answers to these questions as security answers to access accounts, or worse — passwords.
- **Clicking with caution** – Most malware is spread through email attachments. Users need to take the time to read emails and check their legitimacy before clicking on links or attachments. Also, curiosity killed the cat — if you aren't expecting an email from Amazon with a tracking number — it's likely a fraud and before clicking "just to see what it is" — delete! Why? Because it's likely malware.
- **Better password protection** – This is basic knowledge, but is worth saying again. Use advanced passwords that include an upper case, lower case, symbol, and number — and do not use the same password for every account you have under the sun. You should also not keep these passwords stored in a Word document or Post-It on your PC. All of these, are examples of poor password management.
- **Be selective about who you give your data to** – This goes for creating website profiles, registering for coupon deals, and storing your payment information on various retail sites. Although it may be convenient to store the payment data for faster checkouts in the future, you're also releasing that information to a third party that may or may not be able to keep it secure. That is the risk you take. This is the same risk users take by sharing their email addresses, names, birth dates, and more, on various websites.

- **Keep your systems updated** – this includes third-party applications and your operating systems. Updates often patch known vulnerabilities. If you opt not to update, you're leaving these security gaps open to hackers.
- **Deploy an application whitelist security solution** – This will avoid any malicious programs from executing on your device, keeping it malware-free.

Again, once you hand your data over to a third-party, you are trusting them to keep it secure. However, you too must be cognizant of how you're protecting your data and safeguard it accordingly. If you have any more suggestions, feel free to drop a comment below!

IRS Issues Warning – Watch Out For Fraudulent Tax Emails: Scammers Portray IRS in Latest Phishing Scam

Earlier this week, the IRS issued a warning to tax payers regarding a fraudulent email that has been impersonating the agency. The email includes tax transcripts, in an attempt to get the users to click on the documents, which contain malware. The biggest risk would be employees clicking on these emails on company networks. By doing so, the malware would spread network-wide.

The scam email includes an attachment labeled "tax account transcript" or something similar, with a subject line using some variation of the phrase "tax transcript."

According to KLFY News 10, this malware, known as Emotet, generally poses as specific financial institutions in its effort to trick people into opening infected documents. This time, they've portrayed the IRS. Cyber security experts have labeled Emotet one of the most costly and destructive malware variants in the wild.

Proceed with Caution

The IRS has the following suggestions if you receive this email scam:

1. Do not open the email or attachment.
2. Delete or forward the email to phishing@irs.gov.
3. If an email goes to your business, notify the company's technology professionals.

The bottom line – the IRS does not, and will not, send out unsolicited emails. Therefore, if you receive an unsolicited email claiming to be from them– do not open it, it is a scam.