Social Media Breaches So Far in 2020

Devolutions

THIS YEAR WE HAVE SEEN SEVERAL HIGH-PROFILE SOCIAL MEDIA DATA BREACHES

There are still a few months left in 2020, but already this year we have seen several **high-profile social media data breaches, including:**

In February, **Twitter suspended a large network of fake accounts that were used to match phone numbers to users.**

In June, the social media marketing firm Preen.Me disclosed that the **personal data of an estimated 100,000 social media influencers had been leaked**. The same breach also led to over 250,000 social media users having their data exposed on a deep web hacking forum.

In July, the Twitterverse was thrown into chaos when the accounts of some of the world's best-known personalities,

such as Barack Obama, Jeff Bezos, Elon Musk, and Bill Gates, were compromised. Hackers targeted a **small number of Twitter employees** through spear **phishing attacks**, in order to drive traffic to Bitcoin scams.

In August, researchers from Comparitech revealed that a **database of nearly 235 million social media profiles connected to Instagram, TikTok, and YouTube were exposed**, and unprotected by passwords or any other type of authentication.

In August, YouTube **took down 2 million channels and 51 million videos** over scams.

The Hidden Dangers of Social Media

The same thing that makes social media so popular is **also what makes it so risky**: people believe they are communicating with people they know (or if they don't personally know them, then at least they trust them), and as such they **let their guard down**. As pointed out in a New York Times article: "The human error that causes people to click on a link sent to them in an email is exponentially greater on social media sites…because people more likely consider themselves among friends."

Tips for Staying Safe

Many of you will find these tips "common sense" — but as we all know, sometimes common sense isn't all that common; especially for non-technical business users, who unlike you are not hyper-aware of how dangerous the cyber threat landscape has become. **Here is what to keep in mind** and to pass along to your colleagues, clients, family members, and **everyone else who wants to stay safe**:

- **Never click on suspicious messages or links**, even if they appear to be from someone you know.
- **Never post personally identifying information (PII) across any social media platforms**. Hackers regularly mine this information in order to build profiles of potential victims, as well as glean hints for security check answers (e.g. city where you were born, name of your first pet, name of your high school, etc.).
- **Always use unique, strong passwords (or passphrases) for each of your social media accounts**. An estimated 81% of data breaches are the result of weak passwords.
- **Use 2FA/MFA for all of your accounts.**
- **Use a reputable password manager.**

- **Never share passwords with colleagues, friends, or family members**. Yes, it may be convenient, but it's not safe!
- **Try not to log into social media accounts while using a public Wi-Fi access point**. If this is impossible, then use a reputable VPN to encrypt your data and mask your identity.

Cybersecurity Training

We also recommend providing your employees with **cybersecurity training**, which includes (but is not limited to) **safe social media usage**. Since in-person training is a challenge these days, we suggest an **online cybersecurity training platform** that can be accessed by employees from anywhere, including their home office. One of the key benefits of an online portal is that **supervisors and managers can monitor each employee's progress**, and **highlight areas that need additional training**. Learn more here.

Share Your Advice

What are you doing to stay safe while traveling across the social media landscape? Please share your tips and warnings, so that we can all minimize the risk of being the next hacking victim.