COLOR OF CHANGE
DIGITAL DEFENSE GUIDE

DO YOU THINK YOUR DATA WAS STOLEN?

Color Of Change Best Practices to Protect Yourself Online

During the 2020 election and COVID-19 pandemic, bad actors used stolen data to target Black neighborhoods with false voting and health messages because it helped them single us out. Studies show that Black communities are disproportionately targeted by scammers after data breaches. As a part of our Black Tech Agenda, Color Of Change believes that Black people must have individual control over their digital lives. We are committed to making sure Color Of Change members have the necessary tools and strategies if a data breach happens to them.

COLOR OF CHANGE | BLACK TECH AGENDA

Red Flags You've Been Compromised

- Unexplained charges on financial statements
- New accounts you didn't open appearing on credit reports
- Denied credit applications when you have good credit
- Missing mail or unexpected password reset emails
- A mailed notice claiming your data was part of a breach.

Four Steps To Take Immediately

1. Understand What Was Compromised

Data breach notification letters often tell you what types of sensitive information may have been stolen. Different types of breached data require different responses:

- **Social Security Number:** Highest risk — immediate credit freeze needed
- **Credit/Debit Card Numbers:** Contact your bank immediately
- **Email/Password:** Change passwords on ALL accounts using that email
- **Driver's License:** Alert your state DMV
- **Medical Information:** Contact your health insurance provider

2. Change Your Passwords Immediately

Start with the account that might be impacted, then change passwords for:

- Email accounts (these are gateways to everything else)
- Banking and financial accounts
- Social media accounts
- Any account using the same or similar password

Pro Tip: Use a passphrase instead of a password.
For example: "MyGrandma$Makes_TheBestPies7" is much stronger than "GrandmasHouse123"

3. Enable Two-Factor Authentication (2FA)

(i.e. Two steps to login.)
Two-factor authentication (2FA) requires you to get a confirmation code via text message or email before each login. This adds crucial protection even if someone has your password.

4. Monitor Your Money NOW

Look for signs someone has been poking around in your financial information:

- Check all bank statements
- Review credit card transactions
- Look at payment apps (Venmo, CashApp, Zelle)
- Set up text alerts for ANY transaction
- Every state Attorney General's office has a consumer protection division that provides assistance if you need it.

For more information visit coc.is/digitaldefenseguide