


Data Breach: Steps to Keep Your Business Safe !



www.digitaltechpartners.com

“ *CYBERSECURITY IS
EVERYONE'S JOB
INCLUDING YOURS* ”





Data breach is an incident where information is stolen from a system without the knowledge or authorization of the system's owner. A big or small organization may suffer a data breach.

Stolen data may involve sensitive, proprietary, or confidential information such as credit card numbers, customer data, trade secrets, or matters of national security.



Data Breach Consequences

1. Revenue Loss

Significant revenue loss as a result of a security breach is common. Studies show that 29% of businesses that face a data breach end up losing revenue.

2. Damage to Brand Value & Reputation

A security breach can impact much more than just your short-term revenue. The long-term reputation of your brand is at stake as well.

3. Loss of Intellectual Property

Loss of revenue and damaged reputation can be disastrous. In some cases, hackers will also target designs, strategies, and blueprints.



Data Breach Consequences

4. Hidden Costs

Surface-level costs are just the beginning. There are many hidden costs related to breaches that includes legal fees, PR and investigations and insurance premium hikes.

5. Risk of Legal Action and Litigation

Regulations regarding data protection legally bind organizations to ensure all steps are taken to avoid a leak. When it comes to personal information, this can even lead to class-action lawsuits.



Never Reuse Passwords

- Always Use a different password for each system you access, and make it secure and complex
- Always create unique passwords
- Use a password manager (Eg., LastPass, 1Password, or KeePass) to manage your passwords, and ensure you use a complex passphrase for the password manager.
- Don't use your work username/password combination for personal systems.



Use Multi-Factor Authentication

- ❑ Your employer may require this for your corporate systems, but increasingly it is also available for personal systems. Google Two-Step Verification is available for Android and Apple phones/tablets and provides two-factor authentication to Google applications. For instance, increasingly, work and personal matters intermingle in electronic messages and documents. Multi-factor authentication provides another barrier against having one username and password provide access to multiple systems.



Don't click any email or web links!

1. Banks will never email you a link that asks you to enter your name, social security number, and password.
2. Some bogus emails are obviously fake, full of misspellings and doubtful suggestions. But others look very professional.
3. Your friend sends you a link that you weren't expecting. Don't click it. Remember, the sender's address can be spoofed, or their account hacked
4. Instead of following emailed instructions to call or click, you should generally go directly to your bank's website or call from a number you have (perhaps found on the back of a credit or debit card). Phishing and spear phishing are used to collect data or propagate malware.



Change Your Passwords Regularly

1. Use your password manager, and change your passwords every 90 days
2. If you use the same password for long stretches of time, you increase the risk of someone guessing your password.
3. Limits breaches to multiple accounts
4. Prevents constant access by the hacker if the account is breached
5. Protect against possible attacks against your company or yourself



Practice Safe Wi-Fi

This applies at coffee shops, train stations, airports, shopping malls, and anywhere else with “free” Wi-Fi.

1. Turn off automatic connectivity
2. Delete known public access points when complete
3. Use a VPN on secured public Wi-Fi
4. Make sure you connect to secure websites (TLS/HTTPS)
5. Confirm the secured Wi-Fi is authentic and not a fake Access Point.
6. Keep your Firewall enabled and Anti-Virus up to date
7. Update your credentials if exposed on public Wi-Fi
8. Use multi-factor authentication for logins where available



Practice Safe Wi-Fi

- Don't connect to unsecured Wi-Fi
- Don't access banking and financial information
- Don't shop online or unnecessarily expose personal identifiable information
- Don't allow file sharing on the network
- Don't leave your device unattended in public



Keep Your Devices Safe & Consider Their Contents

- Stay alert in public spaces
- Don't leave your devices in an unlocked vehicle, even if the vehicle is in your driveway or garage, and NEVER leave it in plain sight
- Never leave a meeting or conference room without your devices
- Lock your device in a safe place when not in use or use a cable lock that wraps around a desk or chair leg
- BE AWARE that if your computer is stolen, automatic log-ins can make it easy for a thief to send inappropriate messages with your account. Use password protection and require a person to log in every time the computer goes to sleep or powers down.



Keep Your Devices Safe & Consider Their Contents

- If you lose a device, do you have the ability to wipe its contents remotely?
- BACK UP YOUR INFORMATION using cloud-based storage or on portable media such as a CD, DVD, flash drive, or other backup media.
- Consider using secure cloud storage services, or keeping your data on corporate servers, and accessing it remotely, rather than downloading it locally.
- Know the location of your phone, laptop, etc. Know whether you've set up "Find My iPhone"—or a similar remote location tracking app or service



Best Practices for Patches & Software Updates

- Enable automatic software updates whenever possible. This will ensure that software updates are installed as quickly as possible.
- Do not use unsupported EOL software.
- Always visit vendor sites directly rather than clicking on advertisements or email links.
- Avoid software updates while using untrusted networks.



Remember the Physical World!

- ❑ Walking away from your computer to get a cup of coffee? Lock the screen. Put a lock code on your cell phone. Don't leave devices unattended in public spaces—you risk their physical theft, and exposing sensitive company information.
- ❑ Bank statements? Credit card bills? Utility bills? If you're not keeping them, don't just throw them away, shred them. At your office, don't throw away anything that includes company information, such as sales figures, contact information, and marketing plans. Shredding should be your default option. Harvesting information from improperly disposed of paper is one form of information gathering used for identity theft or systems breaching.



Remember the Physical World!

- Don't leave devices unattended in public spaces—you risk their physical theft, and exposing sensitive company information
- Always Lock the screen. Put a lock code on your cell phone.
- Shred Bank statements, Credit card bills, Utility bills.
- Shred any documents that includes company information, such as sales figures, contact information, and marketing plans. Harvesting information from improperly disposed of paper is one form of information gathering used for identity theft or systems breaching.



Notify Early

- ❖ If you think a breach or other failure has occurred, talk to somebody, such as your computer security officer or CIO, or call your bank's fraud hotline. The sooner an incident response starts, the greater the chance of managing the incident successfully and minimizing any damage. The Verizon DBIR mentioned earlier also notes that attackers who get into a system can be there for up to 205 days on average before their presence is known. That number can be brought down through vigilance and reporting anything that appears unusual. Perhaps your user account was locked out when you got to work today. It may, or may not, mean something.

For more info, Contact



Digital Tech Partners, Inc.

63 Tremont Street, Taunton

MA 02780

■ jdanahey@digitaltechpartners.com

■ www.digitaltechpartners.com

■ 774-488-9235

■ 339-970-3556 x101

Or Schedule your appointment [Here](#)



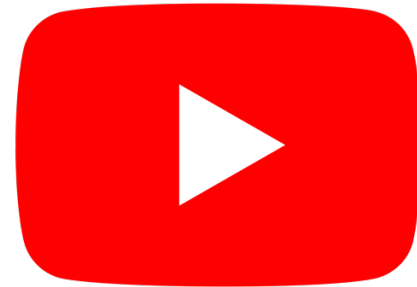
Follow us on Social Media



[Facebook](#)



[LinkedIn](#)



[YouTube](#)