How to Recover from Password Exposure

There are multiple ways that your password can be exposed to unauthorized parties:

1. Passwords are sometimes openly “stored” for convenience in electronic or paper documents. Your password will be exposed if the document is lost or stolen or the electronic document is accessed.
2. Phishing attacks attempt to convince you to enter your password willingly into a website that harvests it for sale or use. If you don’t detect the attack, your password will be exposed.
3. You, your employer, or any organization you interact with digitally can experience a breach.
4. Password-related technologies such as browsers remembering passwords, browser extensions, password manager tools, or even Apple’s Keychain can experience a breach.

You will typically discover breaches that may affect you through traditional and digital news media or directly from the organization that experiences a breach if they are required to notify you. You can also purchase various dark web monitoring services to receive notifications. Some free tools and services allow you to check for yourself or may proactively notify you that you’ve been affected, such as:

- ';--have i been pwned? allows you to search across information about multiple breaches to determine if your e-mail address was included.
- Apple can send notifications to iPhone (see the Detection of Compromised Passwords feature) and Safari browser users.
- Google can send notifications to Chrome users and provides a Password Checkup tool as a follow-up resource.

This blog focuses on breaches that may occur when a password manager tool experiences a security incident that exposes user password data.

In August 2022, LastPass, a popular password management tool, experienced a security breach. While the company assures users that encrypted password vaults remain secure, some source code and technical information were stolen. This incident raised concerns for many users, leading them to question the platform's security.

If you're a user of any password manager tool and considering a switch, here's what you need to know:

Understanding the Breach

LastPass acknowledges that stolen information from the first incident allowed the attackers to access storage volumes considered adequately protected, amplifying the risk that any associated passwords were compromised. While they sought to assure customers that no customer data was directly accessed, the breach highlights the importance of protecting passwords in the strongest possible way.

You'll want to understand the nature of any breach of your terms. Don't hesitate to contact your current provider through their customer support channels to get clarification on any questions you may have.

So, what should you do next?

1. **Evaluate Your Needs & Risk Tolerance:** Research alternative password managers. Popular options include 1Password, Bitwarden, Dashlane, and others. Consider features like multi-device support, security measures, two-factor or multi-factor authentication support, account recovery procedures, and ease of use. More importantly, assess your risk tolerance for different types of accounts.

   Note that these are examples only; you should assess risk for yourself based on your own needs and tolerance:

   - **Low Risk:** Social media accounts and shopping sites you rarely use and for which you do not store payment details.
   - **Medium Risk:** Standalone email addresses not used for single sign-on or management of higher-risk services.
   - **High Risk:** Banking accounts, financial applications, healthcare portals, cloud storage, and other accounts that interact with your financial life.
   - **Extreme Risk:** Accounts used to support popular single sign-on services such as your Apple ID, Microsoft ID, or Google Account.

2. **Prioritize Based on Risk:** Based on your risk assessment, prioritize actions for your most critical accounts.

Security Approaches Based on Risk

- **Essential (Whether you're moving to a new tool or not.):**
  - Use a strong password for your password manager tool and change it regularly.
  - Enable the strongest multi-factor authentication method available for the tool itself:

        - Weaker methods include e-mail, SMS, or telephone call verification.
        - Stronger methods include using biometric or one-time passcode authenticator apps or devices, such as Google Authenticator or Microsoft Authenticator.
        - The strongest methods available include passkeys and certificates.
    - If supported, ensure that you control encryption keys.
    - Clear all cookies and passwords from your browser.
- **Good:**
    - If you are migrating to a new tool, follow the provided instructions.
    - Use your intended tool to change the passwords for your accounts.
    - If applicable, destroy any files used to export the old passwords from your old password manager tool.
- **Better:**
    - This approach adds an extra layer of security.
    - If you are migrating to a new tool, follow the provided instructions.
    - Consider changing the associated user ID or email address after using your intended tool to set strong passwords for all HIGH or EXTREME risk accounts.
    - If applicable, destroy any files used to export the old passwords from your old password manager tool.
    - Consider establishing multiple browser profiles that have no plugins or extensions (except for any required by your password manager tool) to act as containers for direct use of your EXTREME risk accounts.
- **Best:**
    - This approach will be more secure but requires a substantial time investment.
    - If you are migrating to a new tool, follow the provided instructions.
    - Here, you would change the password for all your accounts (regardless of risk) using the new tool and change the associated user ID and email address for EACH of your HIGH and EXTREME risk accounts to be unique.
    - This approach creates separate login credentials for your most critical accounts, minimizing the impact of a breach on any single one.
    - The drawback of this approach is that you may not be able to use commonly available single sign-on services for your highest-risk accounts.
    - If applicable, destroy any files used to export the old passwords from your old password manager tool.
    - Consider establishing multiple browser profiles that have no plugins or extensions (except for any required by your password manager tool) to act as containers for direct use of your HIGH and EXTREME risk accounts.

Remember:

- Be cautious of phishing attempts.
- Never store your passwords as clear text whether electronic or on paper.
- Choose strong, unique passwords for all your accounts. A password manager can help you generate and store these securely.
- Enable the strongest multi-factor authentication method available to you everywhere.
- And don't forget about other sensitive data that you may have stored in a password manager tool such as financial, account recovery, or even cryptocurrency wallet information. While not covered directly in this blog post, you need to perform a risk analysis to determine what recovery actions you should take. Actions to consider should include changing financial accounts or credit/debit card numbers or migrating to a new cryptocurrency wallet.

The mentioned breach serves as a reminder of the importance of cybersecurity vigilance. By evaluating your needs and risk tolerance and addressing them, you can ensure your online accounts remain protected against even the most capable and determined criminals.