Cara Pemulihan dari Tersingkapnya Kata Sandi

Ada berbagai cara kata sandi Anda tersingkap pada pihak tidak berwenang:

1. Kata sandi terkadang “disimpan” secara terbuka untuk kemudahan di dokumen elektronik atau kertas. Kata sandi Anda akan tersingkap jika dokumen hilang atau dicuri atau dokumen elektronik diakses.
2. Upaya serangan phishing untuk meyakinkan Anda agar dengan keinginan sendiri memasukkan kata sandi ke situs web yang mengambilnya untuk dijual atau digunakan. Jika Anda tidak mendeteksi serangan tersebut, kata sandi Anda akan tersingkap.
3. Anda, perusahaan Anda, atau organisasi apa pun yang terhubung dengan Anda secara digital dapat mengalami pelanggaran.
4. Teknologi terkait kata sandi seperti browser yang mengingat kata sandi, ekstensi browser, alat pengelola kata sandi, atau bahkan Keychain Apple dapat mengalami pelanggaran.

Anda biasanya akan mengetahui pelanggaran yang dapat memengaruhi Anda melalui media berita konvensional dan digital atau langsung dari organisasi yang mengalami pelanggaran jika mereka diwajibkan untuk memberi tahu Anda. Anda juga dapat membeli berbagai layanan pemantauan dark web untuk menerima pemberitahuan. Beberapa alat dan layanan gratis memungkinkan Anda memeriksa diri sendiri atau mungkin secara proaktif memberitahukan bahwa Anda telah terdampak, seperti:

- ';--have i been pwned? memungkinkan Anda mencari seluruh informasi tentang beberapa pelanggaran untuk mengetahui apakah alamat email Anda termasuk.
- Apple dapat mengirim notifikasi ke iPhone (lihat fitur Deteksi Kata Sandi yang Bobol) dan pengguna browser Safari.
- Google dapat mengirim notifikasi ke pengguna Chrome dan menyediakan alat Pemeriksaan Kata Sandi sebagai sumber daya tindak lanjut.

Blog ini fokus mengenai pelanggaran yang mungkin terjadi saat alat pengelola kata sandi mengalami insiden keamanan yang menyingkap data kata sandi pengguna.

Pada bulan Agustus 2022, LastPass, alat pengelola kata sandi yang populer, mengalami pelanggaran keamanan. Meskipun perusahaan meyakinkan pengguna bahwa brankas kata sandi terenkripsi tetap aman, beberapa kode sumber, dan informasi teknis dicuri. Insiden ini meningkatkan kekhawatiran bagi banyak pengguna, sehingga mereka mempertanyakan keamanan platform.

Jika Anda adalah pengguna alat pengelola kata sandi dan mempertimbangkan untuk beralih, berikut ini hal yang perlu diketahui:

Memahami Pelanggaran

LastPass menyatakan bahwa informasi yang dicuri dari insiden pertama memungkinkan penyerang mengakses volume penyimpanan yang dianggap cukup terlindungi, memperkuat risiko kata sandi terkait apa pun dibobol. Meskipun mereka ingin meyakinkan pelanggan bahwa tidak ada data pelanggan yang diakses secara langsung, pelanggaran tersebut menyorot pentingnya melindungi kata sandi dengan cara sekuat mungkin.

Anda akan ingin memahami sifat pelanggaran ketentuan Anda. Jangan ragu untuk menghubungi penyedia Anda saat ini melalui saluran dukungan pelanggan untuk mendapatkan kejelasan mengenai pertanyaan apa pun yang mungkin Anda miliki.

Jadi, apa yang harus Anda lakukan selanjutnya?

1. **Evaluasi Kebutuhan Anda & Toleransi Risiko:** Meneliti pengelola kata sandi alternatif. Opsi yang populer termasuk 1Password, Bitwarden, Dashlane, dan lainnya. Pertimbangkan fitur seperti dukungan multiperangkat, langkah-langkah keamanan, dukungan autentikasi dua faktor atau multifaktor, prosedur pemulihan akun, dan kemudahan penggunaan. Lebih penting lagi, menilai toleransi risiko untuk jenis akun yang berbeda.

   Perhatikan bahwa ini hanya contoh; Anda harus menilai risiko untuk diri sendiri berdasarkan kebutuhan dan toleransi Anda sendiri:

   - **Risiko Rendah:** Akun media sosial dan situs web belanja yang jarang Anda gunakan dan di mana Anda tidak menyimpan rincian pembayaran.
   - **Risiko Medium:** Alamat email standalone yang tidak digunakan untuk sekali login atau manajemen layanan risiko lebih tinggi.
   - **Risiko Tinggi:** Rekening bank, aplikasi finansial, portal perawatan kesehatan, penyimpanan cloud, dan akun lainnya yang berhubungan dengan kehidupan finansial Anda.
   - **Risiko Ekstrem:** Akun yang digunakan untuk mendukung layanan sekali login yang populer seperti Apple ID, Microsoft ID, atau Google Account.

2. **Prioritaskan Berdasarkan Risiko:** Berdasarkan penilaian risiko Anda, prioritaskan tindakan untuk akun Anda yang paling penting.

Pendekatan Keamanan Berdasarkan Risiko

- **Penting (Baik Anda beralih ke alat baru maupun tidak.):**
  - Menggunakan kata sandi yang kuat untuk alat pengelola kata sandi Anda dan mengubahnya secara rutin.
  - Mengaktifkan autentikasi multifaktor terkuat yang tersedia untuk alat itu sendiri:

        - Metode yang lebih lemah termasuk email, SMS, atau panggilan telepon.
        - Metode lebih kuat termasuk menggunakan biometrik atau perangkat atau app autentikator kode sandi satu kali, seperti Google Authenticator atau Microsoft Authenticator.
        - Metode terkuat yang tersedia termasuk kunci akses dan sertifikat.
    - Jika didukung, pastikan Anda mengontrol kunci enkripsi.
    - Hapus semua cookie dan kata sandi dari browser Anda.
- **Baik:**
    - Jika Anda bermigrasi ke alat baru, ikuti petunjuk yang diberikan.
    - Gunakan alat yang dimaksud untuk mengubah kata sandi akun Anda.
    - Jika berlaku, musnahkan file yang digunakan untuk mengekspor kata sandi lama dari alat pengelola kata sandi lama Anda.
- **Lebih Baik:**
    - Pendekatan ini menambah lapisan keamanan ekstra.
    - Jika Anda bermigrasi ke alat baru, ikuti petunjuk yang diberikan.
    - Pertimbangkan mengubah ID pengguna atau alamat email yang terkait setelah menggunakan alat yang dimaksud untuk mengatur kata sandi yang kuat untuk semua akun risiko TINGGI atau EKSTREM.
    - Jika berlaku, musnahkan file yang digunakan untuk mengekspor kata sandi lama dari alat pengelola kata sandi lama Anda.
    - Pertimbangkan untuk membuat profil multi-browser yang tidak memiliki plugin atau ekstensi (kecuali diwajibkan oleh (alat pengelola kata sandi Anda) untuk bertindak sebagai wadah penggunaan langsung dari akun risiko EKSTREM Anda.
- **Terbaik:**
    - Pendekatan ini akan lebih aman tetapi memerlukan investasi waktu yang substansial.
    - Jika Anda bermigrasi ke alat baru, ikuti petunjuk yang diberikan.
    - Di sini, Anda akan mengubah kata sandi untuk semua akun Anda (apa pun risikonya) menggunakan alat baru dan mengubah ID pengguna dan alamat email yang terkait untuk SETIAP akun risiko TINGGI atau EKSTREM agar unik.
    - Pendekatan ini membuat kredensial login terpisah untuk akun Anda yang paling penting, meminimalkan dampak pelanggaran satu demi satu.
    - Kekurangan dari pendekatan ini adalah bahwa Anda mungkin tidak dapat menggunakan layanan sekali login yang umum tersedia untuk akun risiko tertinggi Anda.
    - Jika berlaku, musnahkan file yang digunakan untuk mengekspor kata sandi lama dari alat pengelola kata sandi lama Anda.
    - Pertimbangkan untuk membuat profil multi-browser yang tidak memiliki plugin atau ekstensi (kecuali diwajibkan oleh alat pengelola kata sandi Anda) untuk bertindak sebagai wadah penggunaan langsung dari akun risiko TINGGI dan EKSTREM Anda.

Ingat:

- Hati-hati terhadap upaya phishing.
- Jangan pernah menyimpan kata sandi sebagai teks biasa, baik secara elektronik maupun kertas.
- Pilih kata sandi yang kuat dan unik untuk semua akun Anda. Pengelola kata sandi dapat membantu Anda membuat dan menyimpan kata sandi ini dengan aman.
- Mengaktifkan autentikasi multifaktor terkuat yang tersedia untuk Anda di mana saja.
- Jangan lupa juga tentang data sensitif lainnya yang mungkin Anda simpan di alat pengelola kata sandi seperti keuangan, pemulihan akun, atau bahkan informasi dompet mata uang kripto. Meskipun tidak dibahas secara langsung dalam postingan blog ini, Anda perlu melakukan analisis risiko untuk menentukan tindakan pemulihan yang harus Anda ambil. Tindakan yang perlu dipertimbangkan harus termasuk mengubah akun keuangan atau nomor kartu debit/kredit atau beralih ke dompet mata uang kripto yang baru.

Pelanggaran yang disebutkan berfungsi sebagai pengingat pentingnya kewaspadaan terhadap keamanan siber. Dengan mengevaluasi kebutuhan Anda dan toleransi risiko serta penanganannya, Anda dapat memastikan akun online Anda tetap terlindungi dari pelaku kejahatan yang paling kapabel dan gigih.