メールアドレスの漏洩チェック等

JJ1SXA/池

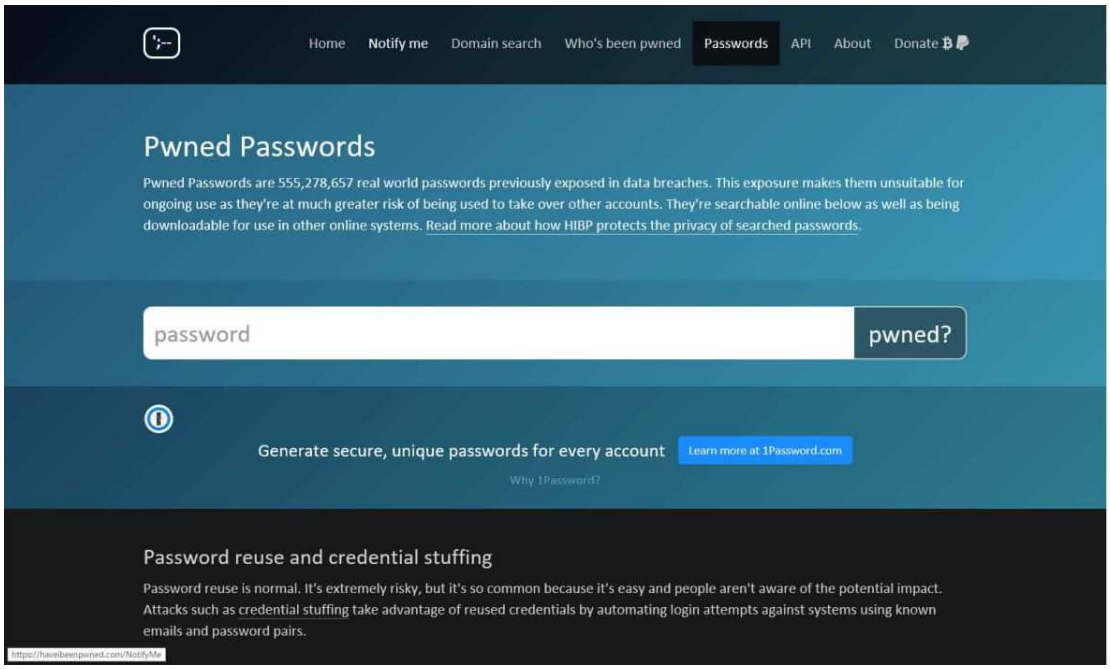
メールアドレスの漏洩チェックは、ファイアーフォックスモニターがFBです、ブラウザをファイアーフォックスに切り替え、「https://monitor.firefox.com」のサイトに移動、アドレスを入力して、「データ侵害を確認する」ボタンを押すだけ。

漏洩していなければ、「このメールアドレスは0個の既知のデータ侵害があります」と表示され、漏洩していると、「このメールアドレスは2個（例）の既知のデータ侵害があります」と表示されます。

クロームでも、IDやパスワードの調査ができます、Chrome拡張機能は、クロームブラウザで「https://chrome.google.com/webstore」を開き、「Password Checkup 拡張」で検索、見付かったら、「chromeに追加」ボタンを押すと、クロームの画面右上に、下図のような「アイコン」が常駐する。

クロームが記憶していたり、サイトで入力したりしたユーザー名（ID）やパスワーソについて漏洩の情報があれば、警告を表示する。

パスワードの漏洩もチェックしましょう、「https://haveibeenpwned.com/Passwords」のサイトを開き、「パスワード」を入力、右隣りの窓の「pwned?」をクリックするだけ。



漏洩が無ければ、「Good news-no pwnage found!」と表示される、漏洩があると、「Oh no-pwned」と表示される。
パスワードの漏洩が確認できれば、即、パスワードの変更は当然のこと。

現在悪徳業者は、「名簿業者から入手する」、「マルウエアに感染させて情報を盗む」、「ウエブ上に掲載された情報を取得」、「ウエブサイトで入力させる」、「総当たり攻撃でアドレスを生成する」、「クラウドや企業のサーバーを攻撃して盗む」等々の手口でアドレスを入手している。

メールアドレスを盗まれないためには、「マルウエア対策は確実に」、「アプリの権限にも注意」、「ウエブやSNSで公開しない」、「怪しいサイトに登録しない」、「簡単なアドレスは使わない」等の注意が肝要のようです。

メールアドレスが漏れないように気を付けていても、何らかの外的要因によりアドレスが漏洩してしまうこともある、つまり、誰でも詐欺メールの標的になり得るのだ。

もしも詐欺メールが届いたら、「無視して捨てろ」が原則、詐欺メールの対応は、「どうすべきか」よりも「やってはいけないこと」の方が重要だ、やってはいけないことは、「メールに返信する」、「添付ファイルを開く」、「リンクをクリックして開く」、「安易に画像を表示する」だ、だが、詐欺メールの見分けは難しい、怪しそうなのは詐欺メールと思った方が良い。

なお、メールは「Gメール」が良さそうだ、「Gメール」の迷惑メールフィルター―は、グーグルが採用する機会学習によって高い精度を誇るようです。

Win10 の標準ブラウザは、「エッジ」ですが、使い慣れた、「IE」を使っている方も多いことでしょう、斯くいう私も、未だに「IE」です。

ただ、「IE」不調時に、即ブラウザを切り替えられるように、「クローム」と「ファイアーフォックス」をダウンロードして、待機させています。

皆さんも、複数のブラウザをダウンロードして、待機させておいて、使用中のブラウザ不調時に切り替えたり、たまには気分転換で、別のブラウザを使ってWEBを見るのも良いものです。

グーグル・クロームダウンロード
https://www.google.co.jp/chrome/

ファイアーフォックスダウンロード
https://www.mozilla.org/ja/firefox/new/