

わるい人たちのpass抜きが流行ってるので注意とか注意とか注意をするにこしたことはない。

最要！WindowsUpdateをする。

抜く手口で主要なものがwindowsとブラウザの「知られている弱いところ」を突いたものなので
ともかくにもあぶでとする。

「知られている弱いところ」はまいくろそふとの高給取りさん達が必死に直してくれているので
わるい人に広く知られる頃には直してもらえます。

「知られてない弱いところ」はpass抜きサイトを作る程度の能力の人たちには見つけれませんので気にしない。

起動したら毎回あぶでとぐらいで可。

タブブラウザを使う。

ActiveXコントロール・ダウンロード

Javaスクリプト・アプレットの許可禁止を一発で切り替えられる。

「web見てただけで被害にギャー」という場合はだいたいこの機能の弱いところを突かれてます。
両方禁止にしといて必要なときに許可する、みたいにつかうべし。

ちょっとむつかしいかもしれないがこれを覚えておくと
普段www生活の危険性もだいぶ減るのでちょっとがんばってみよう。

PeerGuardian2を使う。

「リネージュ資料室」でぐる。

ガイド>セキュリティ対策>基本の対策>IPフィルタ

全部読めとはいわねえ！のでとりあえずダウンロードして「危険IP」のところのtxtアドレスで
リスト追加してください。これで危険サイトは有無を言わずみれねえ。

こっちの情報も奴らに送れねえ。エキサイト。

PC起動時に一緒に起動するようにしといて、アップデートボタンを一緒に押せば更に安心。

中国・台湾・韓国においてあるサーバにはアクセスできなくなるので(wikipediaとか)
どうしても必要のあるときは「一時的に許可」とか駆使してください。

ウィルス対策ソフトを使う。

実はpass抜きにはあんまりやくにたたn

繁殖活動も破壊活動もほとんど無いので検知がし辛いとかいろいろあるようです。

無いよりはあったほうがよろしいのでテキストウにいれておいてください。

そして更新で落ちるFF。

やられたっばかったら。

相手が手を回す前なら大丈夫なこともある。再インスコ。确实安心。
最インスコ終わったら綺麗な体でPOLのパスワード変更しましょう。

ただし確実に「自機がやられているかどうか」は誰にもわからない。
前述のとおりウィルスチェックにも引っかけられない事がおおいのです。
でも他の悪いものも全部出せるので定期的にやましよう。
メンテ時とかに。そして終わらないファイルチェック。

パーティションDとかEとかにお気に入り・アドレス帳・各ドライバ等をまとめておいておくフォルダを作っておくと
あわてずさわがず再設定できます。この機会に覚えるんだ。

もしゲムに被害が出たら

経過を書き留めつつ

GM通報・サポートに電話

県警本部のサイバー犯罪対策なんたらに電話する。
思っきり懲役刑の犯罪なのでちゃんと電話。重要。

GM呼べないサポート空いてないなんて時は先にサイバーなんたらでもいいです。
とにかく連絡。後で交渉事になっても不利は無いのでまず連絡。