ネット社会の安全性について

・近年のネット関連の事件

まぁ、言うまでもなく無数にありますが、よく聞くような、出会い系関係、掲示板に書き込んで云々という話は割愛します。被害者(？)の行動に問題があったのは明らかなので。他には、チェーンメールとかでしょうか。

さてこんな話題はさておき、最近メジャーなのは何と言っても個人情報を巡る事件でしょう。LINE、Facebook、Twitter……etc.といった SNS によるものが話題に挙がりがちですが、本人認証のページを偽装したり、正規の企業名を装って、「～のため認証が必要です。リンク先に ID とパスワードを入力してください」といったメールが送られたり、被害者に非はなくとも個人情報の管理者が第三者に情報を売ってしまったりと多種多様に渡ります。「それがどうした」と言われると、答えに窮しますが、「要は大抵の場合、基本的なことをすれば特に問題ない」ということを言いたいわけです。

・基本的なことって？

① 最低限の常識を持つ。(個人情報をやたら書き込まない、とかワンクリック・ダブルクリック詐欺の知識とか、そういう類です)
② ファイアウォールと共に、総合的なウイルス対策ソフト（ウイルス対策サービス）を用いる。
（弊害は多いですが、一般的にはメリットの方が多いでしょう）
③ ソフトウェアは常に最新の状態にする。(保証の切れた OS やソフトは特殊な目的がない限り使わない方がいいでしょう。最新が最良かと言われるとそうでもないのですけれども)
④ パスワードや個人情報などを書いたメモをその辺に置いたり、丸めてゴミ箱に入れたりしない。
（ゴミ箱は安全みたいな認識だと思いますが、適当に破いたりすることを勧めます）
⑤ メールはフリーメールアドレスを使うようにする。(ダウンロードしない限り、メール関連のウイルスとは無縁でいられます。だからといって怪しげなサイトは登録しないのが一番です)
⑥ ツールやフリーウェアは信用できるサイトからしか極力ダウンロードしない。
⑦ パスワードは英字と数字を両方使ってなるだけ長く予測しにくい文字列にする。

⑧ ネットワークを通じた自分の行動を完全に隠蔽するのは不可能だということを

理解する。
（意外と知らない人が多いようですが、諜報機関やそれに匹敵する技術を用いれば、履歴やキャッシュが残っていなくてもユーザーの情報は筒抜けです。また通信情報などを覗かれる可能性もあります。というか、専用のツールを使えば私のような素人でも情報を閲覧できる場合もあります。だからどうって訳でもありませんが、後ろめたいことはしないほうがいいかなと）

・ネット犯罪でよく聞く用語集

知っていたからといってどうなるって訳でもないのですが、紹介でも。
・マルウェア……悪質なプログラム全般を指します。
・ウイルス……広義は、他ＰＣに広まっていき、何らかの迷惑行為を行うもの、
狭義は、実行ファイルなどが起動するたびにそれに感染するもの
・ワーム……独立性があり、自己増殖するタイプのソフトウェア。他 PC に通信経路を使って広がることが多く、発見が困難です。
・スパイウェア……データを破壊しない代わりに、情報を抜き取るソフト
無料配布のツールなどに混入していたりします。急に動作が重くなったら最近導入したツールを疑うといいかなと。
・トロイの木馬……PC にバックドア(裏口)を仕掛けたり、PC を遠隔操作可能にしてしまうもの。ツールや海賊版に混入されているものが殆どです。
・ＩＰアドレス……世界中で重複しない PC や通信機器に割り当てられた識別番号。DNS システムによってドメイン名やホスト名といった文字列に変換されて運用されています。個人情報といえばそうなのですが、隠すのが面倒なため一般的に隠蔽する人は少ないです。
（ですが、IP アドレスを知られることが不正アクセスに繋がったりすることも考えられないことはないので、不安ならプロキシサーバー等を利用するといいでしょう）

・まとめ

私の母親などは「ネットは怖いから最低限しか使わない」と申しておりましたが、ネットワークシステムというのは近年に発達、普及した素晴らしい技術です。これらを使わずに済ますわけにはいきません。どう頑張っても犯罪に巻き込まれることはありますし、真の意味で安全を保障する方法なんてありませんが、それを理解したうえで、そこそこ安全な方法でほどほどにネットワークライフを楽しんでいただければと思います。