

## Security Wisdom

**“The art of progress is to preserve order amid change, and to preserve change amid order.”**

*Alfred North Whitehead*

**“An ounce of prevention is worth a pound of cure.”**

*-Benjamin Franklin*

Assess the risks involved with using technology *beforehand*. The time and expense involved in cleaning up a system after a compromise, or in cleaning up your credit history after identity theft is *huge* by comparison.

**“Tis easy to see, hard to foresee.”**

*-Benjamin Franklin*

Determining which risks are relevant or probable takes effort, and those who are lazy tend to avoid an objective analysis and accept higher levels of risk. Better set time and money aside for future incident cleanup ...

**Don't accept “candy” from strangers**

Do not open email attachments or click on web links from someone you don't know.

**Beware of the “wolf in sheep's clothing”**

Question *unexpected* email attachments or web links, even if from someone you *do* know. The Sobjig.F worm, for example, successfully exploited people who were too trusting.

**Trust – the foundation of a relationship**

It will help *others* if you have a reputation for only circulating business-related documents that they expect (call ahead – let the recipient know that an attachment is coming if it was not requested), and for using a unique style, opening, closing, or signature. Email that breaks a pattern will raise suspicion.

**It could happen to you**

Macintosh users - do *not* attempt to open email attachments as a diagnostic technique, believing that if it is harmful it only affects PC's and not Macs. A good Mac or multi-platform virus could be on the horizon, and we are ripe for a disaster if Mac users feel immune.

**If it sounds too good to be true, it probably is**

Delete email with unsolicited advertisements, free gifts, notifications from secret admirers, and “get rich” or “you've won” schemes.

---

## **Nothing lasts forever**

Keep anti-virus software current, and use automatic updating features.

If you administer your own computer, ensure that all security patches for all software are applied in a timely manner.

## **There is no “free lunch”**

Beware of free software downloads. Who can really afford the time to develop sophisticated software in the long term for free? Such software might be bait-and-hook promotions that you will ultimately have to pay for, or it might include spyware.

## **Do it right, or not at all**

Turn off any unnecessary or vulnerable services on the computer - even if you do not use the service does not mean an attacker can't. The success of a number of worms over the years has been due to computers using Windows file sharing.

## **Don't let your guard down**

When you are operating a computer or handling information, what you do can have a profound affect on others. In the Sobig.F incident, the worm spread before anti-virus updates were available from the vendors, and before accurate information was available to assist security staffs; however its rapid spread was primarily due to opening infected email attachments. Consider anti-virus software a “safety net” in case of an accident – don't rely on it to stop everything all the time.