Middletown Thrall Library Reference Department Presents

Protecting Yourself

& Taking Control of Your Information

You and your information are constantly at risk. Sure, that sounds a bit alarmist, but, unfortunately, it's true. What kinds of risks? **Scams**, **identity theft**, **computer viruses**, **privacy issues** – just to name a few. In fact, the number of potential risks goes up daily, thanks in part to ever-changing technologies, unknown problems, and innocent mistakes. What can you do to start protecting yourself and to take control of your information? Hopefully this guide will give you some ideas.

Doing Business

Whether you want to purchase a service, place orders over the Internet, or interact with an unfamiliar business or organization, you should find out all you can *before* offering your home address, telephone number, credit card number, or any other personal information. **Many businesses can be checked through the Better Business Bureau** (**www.bbb.org**).

If you intend to buy something through an **online auction** website such as **eBay.com** (or, as another example, a used books dealer), you should check any relevant **customer feedback** and **ratings**. Try to find out if a business is **legitimate** (not a **fake company**) and that you could **contact** them directly (or **report** them) should that ever become necessary.

If you have any issues or negative experiences with a business or organization, please check the **Web Resources** section at the end of this guide for potentially helpful websites, especially those you can use to **report a situation**.

Examine *any* **online offers** – coupons, contests, messages stating someone left you a small fortune, and other too-good-to-be-true announcements – with great **skepticism**. "Coupon software" (or *any* computer programs promising "free" offers) can contain **malware** or **spyware** – bad things which can **steal your information** or track what you do and where you go online.

Downloading & Internet Security Software

Please **think *before* downloading** and installing any software. Even if you trust a certain website or source, always make sure your **Internet security software** (antivirus, firewall, etc.) is **updated** in case a file contains a **virus** (a *very* bad, often *destructive* program). Software that came with your computer can become obsolete within months unless updated. **An unprotected computer is extremely dangerous to use**.

Please try to **familiarize yourself with your security software** so that you will not easily be victimized by **scareware** (**fake software** or sometimes a **fake website**) ***pretending* to have found viruses** on your computer. Scareware usually tries to prompt you to act (e.g. "click here to remove viruses"), but doing so can cause your computer to *get a virus* or to be taken hostage (kept in a state of false alerts until a credit card number was entered – clearly something you would not want to do). Whenever in doubt, you should contact your computer's manufacturer or the company (Symantec, McAfee, etc.) which created your *real* Internet security software for further guidance on how you might resolve your situation.

E-mail Issues

Millions of potential scams appear in e-mail inboxes every day. Please always be mindful of this. If a message ever asks for your **personal information** (user name, password, account number, etc.), remember it is more than likely a scam! These scams might *appear* to be sent by persons, companies, or organizations you recognize and trust, but the true "source" or "sender" of the message can be easily hidden. This phenomenon is known as "**phishing**" and can be very deceiving.

If a message requesting such information *appears* to come from a bank, Internet provider, college, store or place you frequent, or someone you know, contact that place or person (by telephone if possible) to confirm if a message you received was really sent by that place or person. **Never reply directly to such messages unless you are absolutely sure it's safe**.

Please try to **keep your e-mail address as private as possible**. Whoever gets your e-mail address can **share it with others**, and this can cause problems quickly or eventually. "**Spam**" (unsolicited ads, messages, or simply "junk mail") should never be replied to: use your e-mail service to "flag" or "report" a message as spam and then delete the message. Your e-mail might also support **message filters**, so you can send unwanted messages straight to the **Trash** or **Junk Mail** folder. Look for the **Help** or **FAQ** (Frequently Asked Questions) pages in your e-mail service to learn about options available to you.

E-mail messages can contain one or more "**file attachments**" (often indicated by **an image of a paperclip** in a message) and these often can contain viruses. Especially dangerous message attachments are the ones *appearing* to be the safest to open (e.g. "greeting card," "photos," "document," or "[random file name **.zip**]" or "[random file name **.exe**]"). **Do not reply to the message** or attempt to open it before you can **confirm** (by calling the place or person) the attachments are safe to view.

Computer Hardware & Software Issues

While computers are constantly at risk of viruses, spyware, and malware, computer **hardware** (physical parts) can also break down or become unstable if a computer update (or "upgrade") goes wrong. If you have any **personal files** – **photographs**, **documents**, **family videos**, or **anything else you would never want to lose** – you should **take note of where they are on the computer's hard drive** and learn how to **back up** (make one or more copies) of that important information.

(continued)

Also please be aware that **software** (computer programs), including the very **operating system** (**Windows**, **Mac OS/X**, **Linux**) your computer uses, can, over time, be modified or updated to the point your old files might no longer be **compatible**. This means your ***old files* might not work on *newer* programs or computers**. Likewise, **any information you store on a *newer* computer might not be viewable / accessible on an *older* computer**.

Just because *you* can access a file on your computer does not mean someone else can view the information. Try to learn about different information **file formats** (e.g. a document created/saved in **Microsoft Works .wps**, **Microsoft Word .doc**, **Microsoft Word 2007 .docx**, or **OpenOffice .odt**). See if you can still **open** a file you created on a *different computer* and in *different programs of a similar nature* (as in two different brands or versions of **word processors**). See our ***Computer File Formats*** guide (in the **Awareness** section of our **Publications** page: **www.thrall.org/docs**) for more information.

News and Information Everywhere

We often put our minds at risk through the very information we allow into our lives. Information at any time, from any source, can contain any number of issues: **errors**, **missing details**, **partial** or **biased accounts**, **outdated** information, **opinions**, or **outright lies**. We must be, at all times, **critically aware** and not allow anyone to exploit our **lack of awareness** or **manipulate information in any way that can victimize us or keep us from the truth**. We should **consult multiple sources** and **use different search engines** to attempt to get a more "**complete story**," we can **challenge and expand our own understandings** by taking into consideration **the views of others** (especially those with whom we might disagree).

How can you generally protect yourself from informational issues? Start by **asking questions**, by **not settling for one person's perspective** (however agreeable it seems to be). **Refuse to be lied to**, and **never take a "that's good enough for me" approach when doing research or searching the Internet**. Numerous **fake websites** might be listed in any given set of search results. Dig as far and deep as you can for the facts. Ask a librarian for assistance. It really is worth the effort!

What kinds of questions should you ask? Please visit our Publications page (**www.thrall.org/docs**) and select the **Critical Thinking** option on the menu there for our ***Critical Thinking Skills***, ***Media Checklist***, and other guides.

Please also check out the **News Analysis** section our **Current Interests Center** (**www.thrall.org/current**) for in-depth reporting and **investigative journalism** that can take you past the headlines and hype of **mainstream media sources** and help you see and begin to understand some of the **deeper issues** affecting our world.

Personal Information on Your Computer & Online

Websites can use "**cookies**" (information files) for good and bad reasons. Good reasons include keeping track of when you log into a website (such as a Web-based e-mail account) or put items into a shopping cart at an online store. Bad reasons include **tracking which websites you visit** and what things you click on when surfing the Web. If you have advanced Internet security software, it might be able to **scan and remove cookies**. Your **Web browser** (sometimes under its **Tools / Options** or **Edit / Preferences** menu) usually offers options as to **deleting cookies** when you close the browser. Deleting cookies regularly can be a good way to limit how websites might track you.

There are also "**super cookies**" which use things like the Adobe Flash plug-in to save long-term cookies on your computer. **Not all Internet security software or Web browsers will delete these files**. Special software or plug-ins (such as the **BetterPrivacy** add-in for **Firefox**) can help you find and remove these files.

Beyond cookies, **consider the passwords you use**. Are they **similar**? **All the same?** You should keep **different passwords** for different services you use, and you should **change your passwords regularly** to prevent others from guessing your password and gaining access to things like your e-mail or any online accounts or services you use.

Please pay attention to any **privacy policies** posted at the websites you visit. Before you join, try to determine if your personal information would ever be **shared with third-parties**. If so, you probably want to *reconsider* joining that website.

If you belong to a **social network**, check the **privacy settings** of your account. Should the world see *everything* you write and all your photos? If not, change your settings as soon as possible and **edit or remove pages / posts** of possible concern.

Web Resources: Government Websites & Consumer Organizations

Better Business Bureau – BBB (**www.bbb.org**)	Check businesses and charities, file a complaint.
Consumer Safety Product Commission - CPSC (**www.cpsc.gov**)	Use to report online / international companies.
eConsumer.gov (**www.econsumer.gov**)	Use to report online / international companies.
Federal Citizen Information Center (**www.pueblo.gsa.gov**)	Free publications for consumers.
Federal Trade Commission - FTC (**www.ftc.gov**)	Advisories, news, other information for consumers.
Internet Crime Complaint Center – IC3 (**www.ic3.gov**)	Consumer complaints against cyber crimes.
New York State Attorney General (**www.ag.ny.gov**)	Complaints, alerts, forms, laws, rights, more.
NYS Consumer Protection Board (**www.nysconsumer.gov**)	Consumer alerts and advice.
OnGuard Online (**www.onguardonline.gov)**	Tips / advice on privacy, security, fraud, scams.

For More Information…

Please visit our **Thrall Publications** page (**www.thrall.org/docs**) for more free **Awareness**, **Critical Thinking**, and **Reference & Research** guides. Thrall also maintains a **Consumer Information guide** (**www.thrall.org/consumer**) to help you find advisories, advice, product ratings and reviews, and other resources to help you **empower yourself** as a consumer. Please use these and all your library's resources to help fortify yourself against informational dangers on or beyond the Web.