

PROTECTING YOUR IDENTITY

Recommendations made by:

Maricopa County Attorneys Office Web site
Federal Trade Commission Web site

- Shred documents before you throw them away.
- Do not leave mail in mailbox.
- Do not leave important documents in car.
- Balance checkbook & credit card balances often.
- Keep credit card limit low & have fewer CC's.
- Opt out for prescreened credit cards:
-<http://www.optoutprescreen.com>
- Check Credit Reports regularly at no cost:
-<http://www.annualcreditreports.com>
-877-322-8228
-<http://www.ftc.gov>
- Do not give out personal information via email
-see *Phishing section!*
- Do not open SPAM emails or download files from unknown sources!
- When submitting personal information, make sure you see the 'lock' for SSL. -see *Basic Computer Security!*
- Never toss a computer without a wipe down!
- Install a Firewall!
- Regularly update PC Operating System, Browser, Anti-virus software, Anti-Spyware & firewalls!

Web sites:

- City of Tempe Security Web site @
<http://www.tempe.gov/security/>
- Maricopa County Attorneys Office Web site @
<http://www.endidtheft.com>
- Federal Trade Commission Web site @
<http://www.ftc.gov> ->click on 'Site map'
- The 3 major Credit Bureaus
-<http://www.equifax.com>
-<http://www.experian.com>
-<http://www.transunion.com>

NOTES:

No product is endorsed by the City of Tempe even though some examples may be offered. Tempe takes no responsibility in how this information is used nor for the security of the computers owned and operated by its citizens.

WHAT EVERY HOME PC NEEDS

1. Virus Protection
2. Spyware Protection
3. Firewall Protection
4. Updated Software
5. A driver with common sense

WIFI SECURITY

- ✓ Change the default Administrator password for wireless router.
- ✓ Consider turning off Windows XP Remote Desktop.
- ✓ Consider turning off SSID Broadcast.
- ✓ Consider enabling WEP/WPA data encryption.
- ✓ Consider a MAC based security.

NOTES:

No product is endorsed by the City of Tempe even though some examples may be offered. Tempe takes no responsibility in how this information is used nor for the security of the computers owned and operated by its citizens.

**SECURITY BEGINS
AT HOME!**
**ONLY YOU CAN
PROTECT YOUR
COMPUTER!**

<http://www.tempe.gov/security>

16-June-05



Andrea Gattorna

ITD Training Coordinator
Information Technology Department
City of Tempe

<http://www.tempe.gov/security>

BASIC COMPUTER SECURITY

- ❑ Passwords
 - Use a minimum of 8 characters.
 - Use number and letters.
 - Mix upper & lower case.
 - Deliberately misspell words.
 - Do not use words found in a dictionary.
 - Do not use names of family members or pets.
 - Change often.
- ❑ Web Page Security
 - SSL Secured & 128 Bit Encryption
 - https:// & the 'Lock'
- ❑ Browser Settings
 - IE6->Tools->Internet Options->Security Tab->Custom Level Tab->Cookies
- ❑ -Cookies really do taste good, there not all that bad!
- ❑ Regularly update PC Operating System, Browser, Anti-virus software, Anti-Spyware & firewalls
 - If you have Windows XP, install latest patches and WinXP Service Pack 2 from Microsoft:
 - >Start ->Help and Support ->Keep your computer up-to-date with Windows Update.

NOTES:

PESKY SPAM

Recommendations made by FTC.gov

- ✓ Be very selective when giving out your email address.
- ✓ Check the privacy policy when submitting your email address to a Web site. i.e. deselect checkmarks for lists.
- ✓ Typically do not click on 'unsubscribe' from SPAM email.
- ✓ Use 2 email addresses, 1 personal email address and another for newsgroups & submitting to a Web site.
- ✓ Don't use your full name when creating an email address, use a unique email address to avoid 'dictionary attacks'.
- ✓ Don't allow your email address to display on a Web site.
- ✓ Find out if your ISP has a SPAM Filter, most ISP's do!
- ✓ Use an Email Filter on your PC, i.e. MS Outlook 2003.
- ✓ If you receive SPAM email from friends, they may have a worm/virus or Spyware on their PC.

SPYWARE

- ❑ **Spyware** is installed on your computer with or without your consent; spyware monitors or controls your computer use. It may be used to send pop-up ads, redirect your computer to websites, monitor your Internet surfing, or record your keystrokes, which could lead to identity theft.
 - FTC.gov
- ❑ The clues that spyware is on a computer include:
 - barrage of pop-up ads.
 - hijacked browser with a new Internet home page.
 - new and unexpected toolbars and icons.
 - keys that don't work.
 - random error messages.
 - sluggish or downright slow performance.
 - auto dialer makes long distance call from your PC.
- ❑ How to prevent Spyware installation:
 - Read the 'fine print' when installing software.
 - Avoid 'drive by' downloads because its free.
 - Don't click on links from pop-ups.
 - Don't click on links from SPAM.
 - Keep Security software updated & install a firewall.
 - Install an Anti-Spyware program from a trusted source.

NOTES:

No product is endorsed by the City of Tempe even though some examples may be offered. Tempe takes no responsibility in how this information is used nor for the security of the computers owned and operated by its citizens.

EMAIL PROTECTION

- ❑ **Virus**-The goal of viruses has really changed. Nowadays Viruses may harm your PC or they may not harm your PC in an attempt to steal your identity.
- ❑ **Trojan Horse**-A Trojan Horse *compromises the security of your computer*. Typically it relies on someone emailing it to you or downloading. Trojans are installed under the guise of an entertaining program (i.e. holiday screensavers, free programs downloaded from internet). Once your PC is infected with a Trojan Horse, computer hackers could have complete access to your computer.
- ❑ **Hoax**-a.k.a. an 'Urban Legend'. A Hoax is a false warning about a computer virus. Do not forward a virus warning to friends until you have checked the validity of the claim:
 - <http://securityresponse.symantec.com>
 - <http://us.mcafee.com>

PHISHING

Is someone Phishing for your information?

- ❑ **Phishing** is a high-tech scam that uses spam emails or pop-ups to trick you into disclosing your credit card numbers, bank account info, Social Security number, passwords, or other sensitive information. -FTC.gov
- ❑ The message usually says that you need to "update" or "validate" your account information. It might threaten some dire consequence if you don't respond. The message directs you to a Web site that looks just like a legitimate organization's site, but it isn't.
- ❑ One tactic is to include all legitimate URLs except for the one that clicks through to their collection page where they ask for the sensitive information.
- ❑ Do not reply to any pop-up or email requesting your personal or financial information.
 - If you do, look at the Web site address & call your bank or company to confirm the email is valid.
- ❑ Phishing can also happen by phone!