

## Internet Security Best Practices

For more information on Internet Security please visit <http://TechTeachToo.com>

### Basics

There are no “safe” websites. Any website can be compromised.

Use STRONG passwords where money or sensitive information is involved. They should be 12 characters long and include both numbers and special characters.

Use multiple layers of security software on your computer.

Keep the security software updated.

Scan your computer with security software regularly.

If you have a wireless system, make sure it's set up securely.

### Physical Security

Keep your laptop with you at all times when not at home. Treat it as you would your wallet or purse.

If multiple people use one computer, create user accounts for everyone, including yourself. (Only for Windows users, not for Mac users)

Unless you're a tech-literate power user, create a user account for yourself even if you're the only one using the computer. It will greatly reduce the risk of getting infected.

### Browser Security

Watch URLs to know for sure where you are.

Don't assume a website is what it claims to be unless you've typed in the URL yourself. Even then you might be wrong.

Seeing the lock icon on the address bar or elsewhere on the page only ensures that the data is being transferred securely. It doesn't ensure that the vendor is trustworthy or that the database of customer information is secure.

Never type an important password (leading to money, sensitive information, etc) into a non-encrypted page (one without the lock icon).

Delete cookies, flash cookies, adware and spyware unless you have a good reason to keep them.

Don't allow your browser to remember passwords. When a website, or your browser asks "Remember me?" or "Remember this password?" Say 'No.'

### **Make online payments more secure**

If possible make payments through a 3rd party like PayPal. Fewer vendors will have your credit card number.

If you can't use a 3rd party for payment, use a credit card for online purchases rather than a debit card. Credit cards reduce the liability of the problem if something goes wrong.

For more security when shopping use prepaid credit cards or 'disposable' credit card numbers, also known as 'virtual' credit card numbers.

### **Increase e-mail security**

Be suspicious, if not paranoid, about e-mail attachments and websites.

Don't allow your browser to remember your passwords.

Don't assume that any e-mail is actually from the "From" address.

Delete obvious spam without opening it.

Don't open e-mails with attachments unless you know what the attachment is.

Don't trust unsolicited e-mails.

Never click on links in e-mails. Type the URL into the browser yourself.

### **Final notes**

Backup your data, or your whole system, regularly. There's a lot you can't defend against. A backup of your data or computer will make recovery much easier.

Turn your computer off when not in use. Broadband and an always-on connection can be a dangerous combination.

Nothing is foolproof. Good security practices such as these don't eliminate the risk, but they make you less of a target.