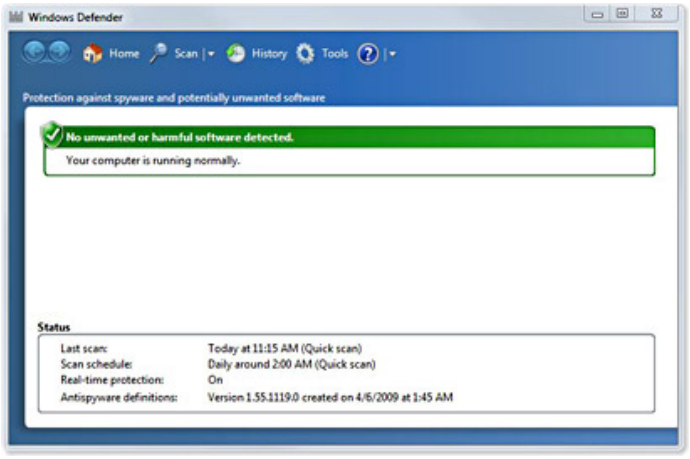
Personal Security Defenses

DEFENSES AGAINST SPYWARE

Spyware needs to be dealt aggressively and here are a few suggestions:

Install Anti-spyware software



Install anti-spyware software, keep it updated (preferably on a daily basis) and be sure that it monitors in real-time and communicates with you regarding what is found and what you should do.

There are both free and for profit versions of anti-spyware. Having multiple Anti-spyware programs is a good idea and is recommended.

Keylogger Defenses

1. Bring your own programs (portable apps) or boot to your own operating system.
2. Check for key loggers in public places before you use the computer.
3. Bring your own computer. This way you use your own protection mechanisms.
4. Use an anti-keylogger or a key scrambler program (stored on your USB drive). You could also use an on-screen keyboard or a password manager program. The idea is to copy and paste instead of type.

5. If you do online banking, subscribe for OTP - One Time Passwords. Most Banks around still make use of the PIN/TAN system. With the PIN you login to your account. The TAN is usually a transaction password which you take from a long list of approved codes which should secure you from fraudulent transactions.
6. A non-technical way of avoiding keyloggers is to just open the page you want to login to and navigate to the login form. Type the first letter of your user credentials and click somewhere else outside the form, so the cursor disappears. Now type a series of random/meaningless characters. Those will not appear in the form, but will still be recorded by the keylogger. Now click back

to the input field and type the second character. Click out again, type a few more random characters. Continue this until you are finished and then login.

USING STRONG PASSWORDS

Strong passwords are a must!

Our passwords are the keys you use to access personal information that you've stored on your computer and in your online accounts. In today's online world, having a strong password is a must. However, the problem with strong passwords is that they can be difficult to remember.

Your password is your first defense AGAINST AN attacker – which could be the person right next to you.

Here are some tips to making a password strong:

1. Combine letters, numbers, and symbols. Make it hard to guess.

2. Use words and phrases (pass phrases). These are easy to remember, difficult for others to guess. If you system does not allow pass phrases (because of an administrator controlled security policy), convert it to a password. For example, the phrase "**I like to eat fish on Friday**" could be made into the following password "**Iltefof**".

3. Use Symbols against words like:

    a. Replace any 'a' with @
    b. Replace any 's' with $
    c. Replace spaces with the percent symbol (%)
    d. Replace any 'o' with 0 (zero)
    e. Replace any 'i' with !
    f. Replace any 'c' with (

    Note: some passwords do not allow symbols, but this does not mean you still cannot use the key that the symbol is on (i.e. #4 key has the $ symbol).

4. Avoid sequences or repeated characters such as "12345678," "222222," "abcdefg," or adjacent letters on your keyboard.

5. Avoid using your login name as a password. Any part of your name, birthday, social security number, or names of your loved ones constitutes a bad password choice.

6. Use a Password Meter, it can test your existing password for strength but also provides guidelines for creating stronger passwords. For example, the "P@ssw0rd" password is rated strong, see image below.

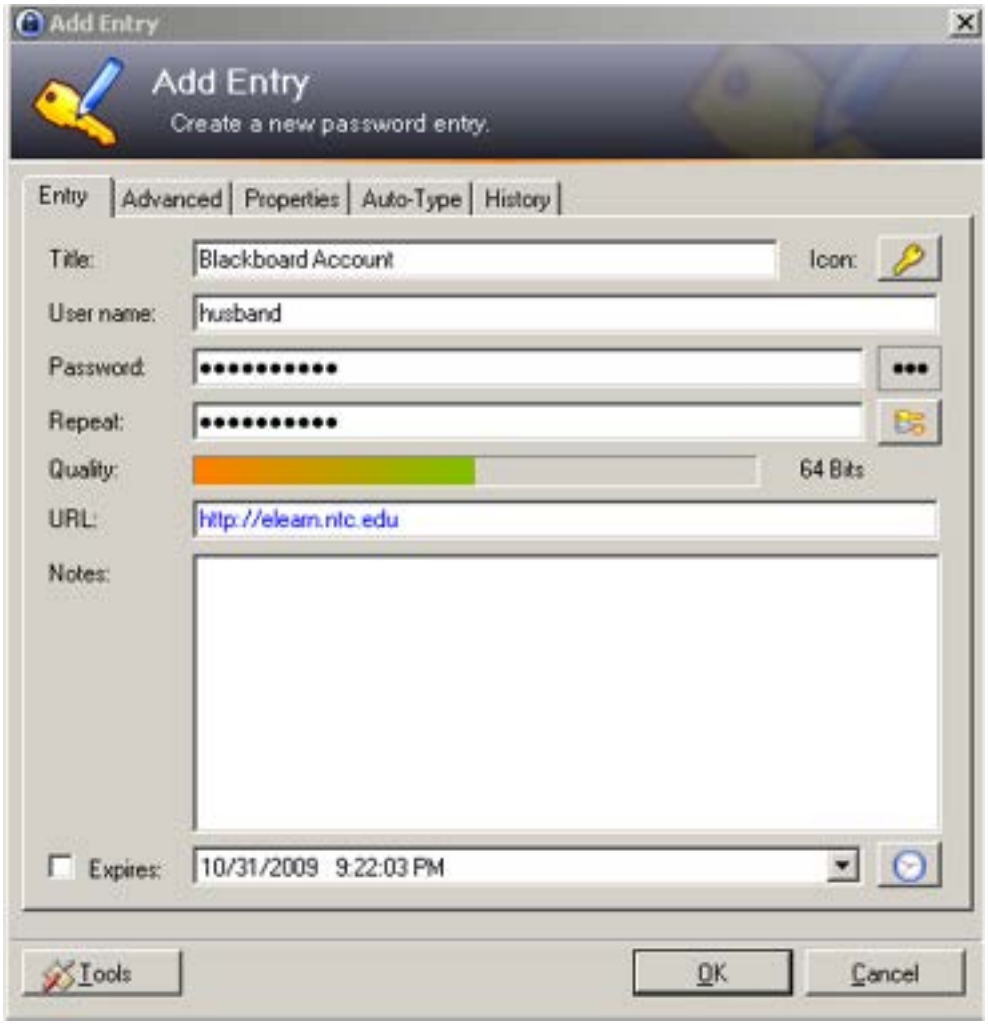
Test Your Password		Minimum Requirements
Password:	•••••••••	• Minimum 8 characters in length • Contains 3/4 of the following items: - Uppercase Letters - Lowercase Letters - Numbers - Symbols
Hide:	☑	
Score:	68%	
Complexity:	Strong	

Additions	Type	Rate	Count	Bonus
Number of Characters	Flat	+(n*4)	8	+ 32
Uppercase Letters	Cond/Incr	+((len-n)*2)	2	+ 12
Lowercase Letters	Cond/Incr	+((len-n)*2)	4	+ 8
Numbers	Cond	+(n*4)	1	+ 4
Symbols	Flat	+(n*6)	1	+ 6
Middle Numbers or Symbols	Flat	+(n*2)	2	+ 4
Requirements	Flat	+(n*2)	5	+ 10
Deductions				
Letters Only	Flat	-n	0	0
Numbers Only	Flat	-n	0	0
Repeat Characters (Case Insensitive)	Incr	-(n(n-1))	2	- 2
Consecutive Uppercase Letters	Flat	-(n*2)	0	0
Consecutive Lowercase Letters	Flat	-(n*2)	2	- 4
Consecutive Numbers	Flat	-(n*2)	0	0
Sequential Letters (3+)	Flat	-(n*3)	0	0
Sequential Numbers (3+)	Flat	-(n*2)	0	0

Legend

Exceptional: Exceeds minimum standards. Additional bonuses are applied.
Sufficient: Meets minimum standards. Additional bonuses are applied.
Warning: Advisory against employing bad practices. Overall score is reduced.
Failure: Does not meet the minimum standards. Overall score is reduced.

7. Use a password storage program that will allow you to use very complex passwords for multiple online username/password combinations. You just need to define the username, password and the URL requiring the password. You will need to use a master password to access the database, and then it is just a matter of drag and drop into the login form. Password storage programs of course can still be used with simple passwords. See image below for an example of such a program.



RECOGNIZING PHISHING ATTACKS

Don't be tricked.

Phishing is just social engineering. To combat phishing tricks you must learn to recognize them.

Click on the link below to learn what Microsoft has to say about phishing.

http://www.microsoft.com/protect/fraud/phishing/symptoms.aspx

Enable Smartscreen in IE8

Make sure you have the Smartscreen filter enabled in IE8.

Click **Tools**, select **Internet Options**, select **Advanced**. Scroll down to **Security** and then click the **Enable SmartScreen Filter** check box to place a check mark by the box if necessary.

This will essentially flag you when you are on a site that is known to be a phishing site.

Click on the link below to get more information.

http://www.microsoft.com/security/filters/smartscreen.aspx

SETTING SOCIAL NETWORKING DEFENSES

Be cautious!

By releasing personal information on social networking sites like Facebook you could possibly be giving an attacker the information he needs to lay the ground work down for a personal attack against you. Lately, employers are using social networking sites of employees or employee candidates to explore the possibility of hiring or perhaps firing.

Click on the link below to get more information on how to make your Facebook experience safer.

http://www.allfacebook.com/facebook-privacy-2009-02

AVOIDING IDENTITY THEFT

Fight back against identity theft.

Take the time and read what the Federal Trade Commission has to say about identity theft – Deter, Detect and Defend.

Click on each icon below in the image below to get more information about deter, detect and defend.

Get a Credit Report

The Fair and Accurate Credit Transaction Act (FACTA) of 2003 contains rules regarding consumer privacy. With this act you have the right to request one free credit report from each of the three national credit-reporting firms every 12 months (or 1 every 4 months).

If you find a problem, then you would need to mail a letter to the credit reporting agency (listed below) for a resolution that may eventually include all of the credit reporting agencies.

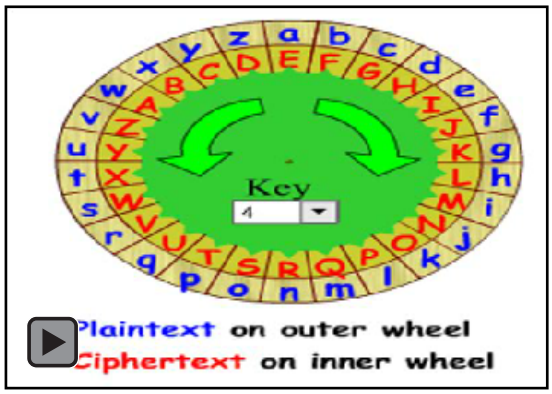
Equifax
P.O. Box 740256
Atlanta, Georgia 30374

Experian
P.O. Box 9554
Allen, Texas 75013

TransUnion
P.O. Box 6790
Fullerton, CA 92834

Cryptography Explained

When you were a kid, you may have used cryptography to relay a secret message to a friend. Let's say for example that you had a hidden treasure and you wanted to give your friend a clue to where it is. You work out a translation scheme that becomes a secret key that only you and your friend know about. You may have used a simple Shift (Caesar) Cipher key to encrypt your message – see image on right.



Let's play! Assume that your secret message or "cipher text" is the encryption stated below:

PSSO YRHIV XLI HSK LSYWI JSV XLI JMVWX GPYI

The same key is used to create the encrypted cipher text as is used to decrypt the text. This is called symmetric cryptography.

Try to decipher the code yourself. Click on the image above to find the answer.

Private Keys in the Real World

You can turn your own documents into cipher text (encrypted data) using a key established by your Windows 7 Professional operating system to encrypt and decrypt the document. Note: you must have your drive formatted NTFS to use encryption.

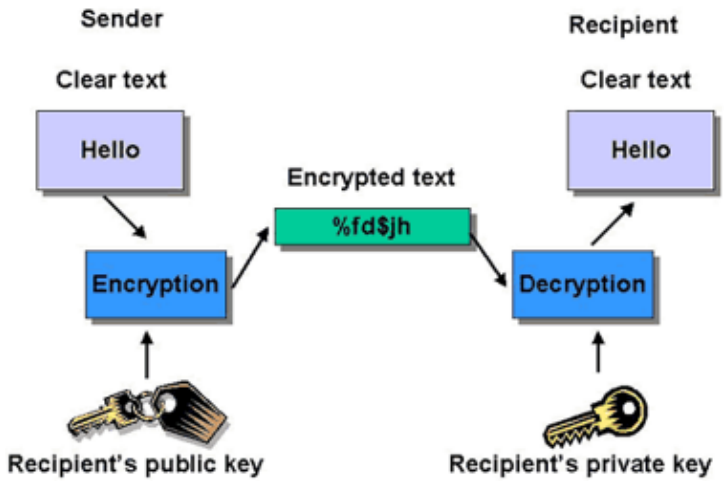
1. Create a folder on your C: drive.
2. Right click on the folder and then select **Properties**.
3. From the properties window select **Advanced**.
4. Check the box next to **Encrypt contents to secure data**.

How do you share the secret key?

The need to share a secret key, which is required for both encryption and decryption, can be a major vulnerability when the key must be transmitted over a network, like the Internet. To resolve this problem asymmetric cryptography was born. This is called Public Key Cryptography.

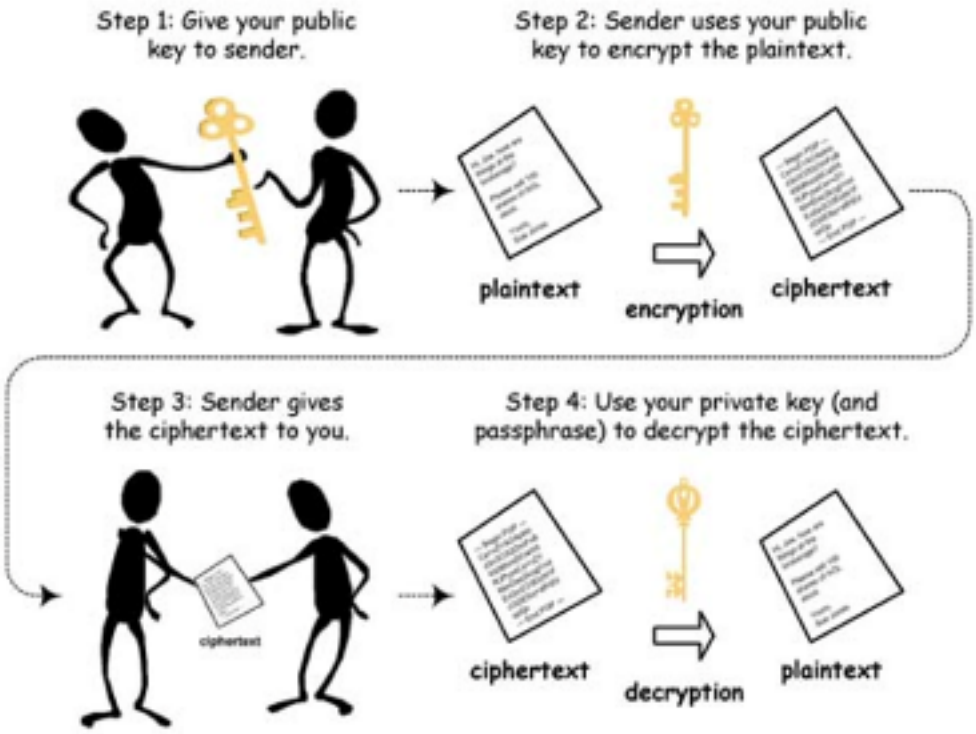
Here's how it works:

Two keys are involved in public key cryptography. They are both mathematically related and work together in such a way that the plain text that needs to be kept secret by encryption (such as a password) is encrypted with one key but can only be decrypted (turned back into plain text) with the other. The key that does the decryption is the one that will be kept private, which means it is not sent on the network. The key that does the encryption is made public and is what is shared on the network. See image below.



Explanation using HTTPS

When you make a secure transaction on the Internet, such as when you purchase something, the security aspect of your transaction is with public key cryptography. Look at the image below.



In this graphic you are the sender. It is your information that has to be encrypted and sent to the server. You will receive a public key from the web server you are connected to. The public key is embedded in a digital certificate that you receive from the web server.

When your browser receives the digital certificate it must first approve the certificate. Once approved, your transaction is encrypted (translated from plaintext to ciphertext) using the public key from the certificate and then sent to the web server. The web server uses its' private key to decrypt the message to plaintext.

You will know when you have a secure connection when the protocol is https and when you have a padlock to the right of your URL.