



# **Internet Security**

**By Vadym Samoylov**

# Introduction

1



**Leading Threats to Computer Security**

---

2

**How protect yourself and your Computer?**

---



**Today online users are faced with multitude of problems. A typical online user is vulnerable to virus, worms, bugs and Trojan horses. They are also facing with phishing of financial information and subjected to invasion of privacy with the multitude of spy ware available for monitoring their surfing behaviours.**

**Users can also faced with malwares that stop or totally destroy their machines render them helpless. These instances only indicate that the Internet is not a safe place for online users. We are constantly vulnerable to hacked sessions, attacks and phishes.**

.

# Leading Threats to Computer Security



## **Viruses/Worms**

Software programs designed to invade your computer, and copy, damage or delete your data



## **Trojan Horses**

Viruses that pretend to be programs that help you while destroying your data and damaging your computer



## **Spyware**

Software that secretly watches and records your online activities or send you endless pop-up ads

# How to protect yourself and your computer?

## To Protect Yourself

1. Use strong passwords
2. Understand email is not secure
3. Recognize phishing attempts
4. Make sure you use secure websites
5. Prevent identity theft

## To Protect Your Computer

6. Use anti-virus software
7. Use anti-spyware software
8. Keep your computer updated
9. Use a firewall
10. Backup your important files

# 1. Use Strong Passwords

---

- ▶ Keep your passwords private and create ones that are hard to “crack”
- ▶ Never share your passwords with friends or be tricked into giving them away



# Protect Your Passwords

- ▶ Do not reveal to others
- ▶ Protect any recorded passwords
- ▶ **NEVER** provide your password over e-mail or based on an e-mail request
- ▶ Do not type passwords on computers that you do not control (trust)
- ▶ Only enter passwords into secure sites

Change your passwords at least once a semester

The screenshot shows a web browser window titled "Bowdoin" with a browser address bar showing "Account Manager :: oblaas" and a page title "Network Operations". The main content area is titled "Passphrase Change" and includes a navigation menu on the left with links for "Passphrase Change", "Email Account Settings", and "Wireless Card Activation". The main text explains that the passphrase must conform to specific security specifications. A list of requirements includes: using a combination of letters, numbers, and symbols; having at least one uppercase letter and one number or symbol; a minimum of 8 characters and a maximum of 30 characters; not containing dictionary words, starting with a dash, or being a name, repeating pattern, reverse of username, palindrome, or sequence of related characters. Below the list, a recommendation suggests using the first letters of words and punctuation in a memorable phrase. At the bottom, there are three input fields labeled "Old Passphrase:", "New Passphrase:", and "Confirm New Passphrase:", followed by a "Change Passphrase" button.

**Passphrase Change**

To ensure that your passphrase is secure, it must conform to the following specifications:

**Passphrase Specifications:**

- Must use a combination of letters (uppercase and lowercase), numbers, and symbols (0-9!@#%&\*~\_~)
- Must use at least one uppercase letter and one number or symbol.
- Must have a minimum of 8 characters
- Must have a maximum of 30 characters
- Cannot contain dictionary words
- Cannot begin with a dash (-)
- Cannot contain part of your name or a repeating pattern
- Cannot be the reverse of your username or your username itself
- Cannot be a palindrome, license plate number, social security number, date, phone number, short number, sequence of keyboard keys, or a sequence of closely related characters.

We recommend that you combine the first letters of each word and any punctuation in a phrase memorable to you (but not easily guessed by others).

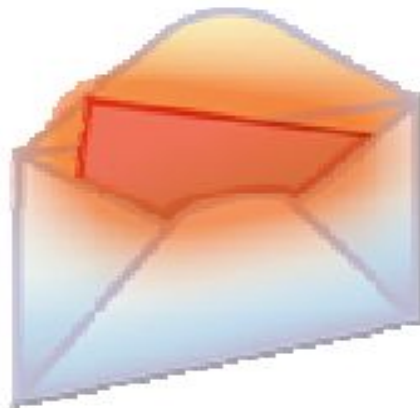
Old Passphrase:

New Passphrase:

Confirm New Passphrase:

## 2. Understand Email is **NOT** Secure

- ▶ Without the use of encryption, email can be intercepted and read without your consent
- ▶ Do not trust that an email came from the person in the “From” field
- ▶ Be wary of attachments received by email – they can contain viruses
  - ▶ Word, Excel, PDF, picture and music files can contain viruses!
  - ▶ An attachment from someone you know can contain a virus





### 3. Recognize Phishing Attempts

- ▶ Mass email sent claiming to be from reputable or trusted organization
- ▶ May include links to a fake website
- ▶ May ask you to reply with your username and password
- ▶ May ask for other personal information (credit card, social security, mother's maiden name, etc)
- ▶ Some are poorly written
- ▶ Generally do not make sense (out of context)
- ▶ Mail may originate from or reply to free email services (Yahoo, Gmail, Hotmail, etc)



## 4. Use Secure Websites

### ▶ Look for:

- ▶ “https://”
- ▶ Yellow lock in location or status bars
- ▶ Blue or green location bar

**!** NEVER enter sensitive information or passwords into unsecure websites

### Firefox Examples



### Internet Explorer Examples



# . Use Anti-virus Software

---



- ▶ Anti-virus software can detect and destroy computer viruses before they cause damage
- ▶ Just like a flu shot, for anti-virus software to be effective, you must keep it up to date
- ▶ AVG

# Keep Your Computer Updated

Install all security updates as soon as they are available

Automatic updates provide the best protection

Be sure to restart your computer after installing updates



# Backup Your Important Files



✓ Keep your critical files in one place on your computer's hard drive so you can easily create a backup

- ▶ Reduce your risk of losing important files to a virus, computer crash, theft or disaster by creating backup copies
- ▶ Save copies of your important documents and files to a CD, DVD, flash or USB drive, or online backup services
- ▶ Test your backups



Thank you for your  
attention and don't forget  
about your safety on the  
Internet!:)