



# 10 Things You Need to Know About Internet Security

Presented by: Steven Blanc – IT Security Officer, Bowdoin College

# Internet Security Versus Internet Safety

---

- ▶ **Security:** We must secure our computers with technology in the same way that we secure the doors to our offices
- ▶ **Safety:** We must act in ways that protect us against the risks and threats that come with Internet use

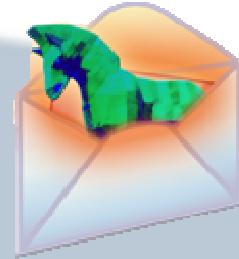


# Leading Threats to Computer Security



## **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



# 10 Things You Need To Know...

---

## 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



# Safety

---



Protecting Yourself



# 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



# Creating Strong, Memorable Passwords

---

## 1. Think of a sentence you can remember

“My son Aiden is three years old.”

## 2. Does the system allow passphrases?

## 3. Convert phrase to password

“msaityo”

## 4. Add complexity

“My SoN Ayd3N is 3 yeeRs old”

“MsAy3yo”

## 5. Substitute some special characters

“MySoN 8N i\$ 3 yeeR\$ old”

“M\$8ni3y0”



# Password Strategies to Avoid

---

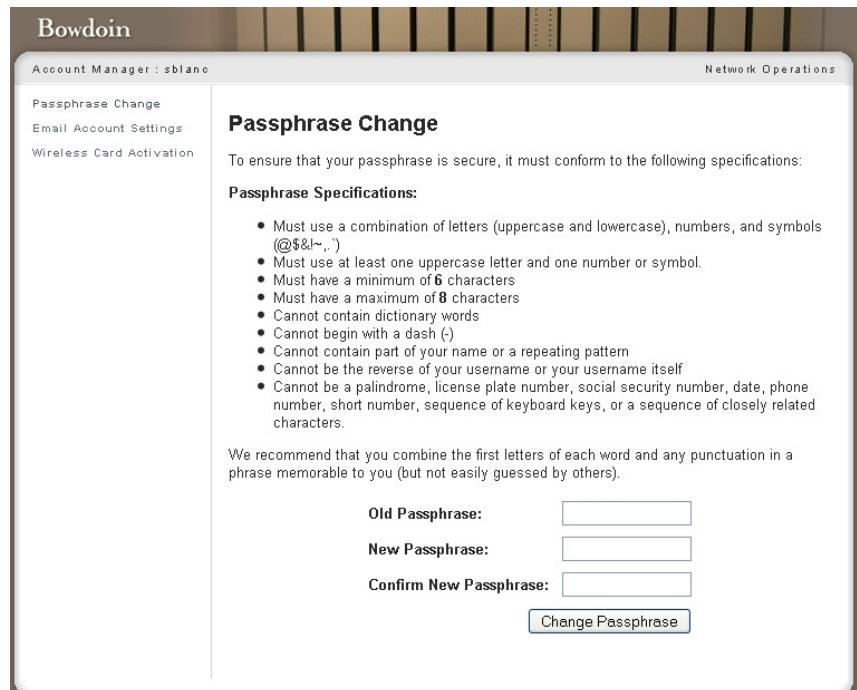
- ▶ Avoid sequences or repeated characters  
“12345678”, “222222”, “abcdefg”, “asdfjkl;”
- ▶ Avoid using only look-alike substitutions of numbers or symbols  
“Mlcr0\$0ft”, “P@ssw0rd”
- ▶ Do not use your login name
- ▶ Avoid dictionary words *in any language*
- ▶ Avoid using the same password everywhere
- ▶ Sticky notes under the keyboard (or elsewhere)



# 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**

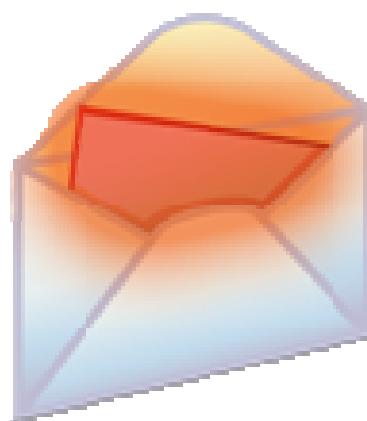


**Bowdoin**

## 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)



**Bowdoin will NEVER request your password be sent by email**



# Phishing – Use “Stop-Look-Call”

---

- ▶ **Stop:** Do not react to phishing ploys consisting of “upsetting” or “exciting” information
- ▶ **Look:** Look closely at the claims in the email, and carefully review all links and web addresses
- ▶ **Call:** Do not reply to e-mails requesting you to confirm account information; call or email the company in question to verify if the email is legitimate



Never email or instant message personal information



## 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*



## 5. Prevent Identity Theft

---

- ▶ Do not give out financial account numbers, Social Security Numbers, driver's license numbers or other personal identity information unless you know exactly who is receiving it
- ▶ Never send personal or confidential information via email or instant message
- ▶ Do not fall for phishing scams
- ▶ Read website privacy statements
- ▶ Order a copy of your credit report from each of the major credit bureaus – You are entitled to one free report from each per year

[www.annualcreditreport.com](http://www.annualcreditreport.com)



# Security

---



Protecting Your  
Computer



## 6. 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

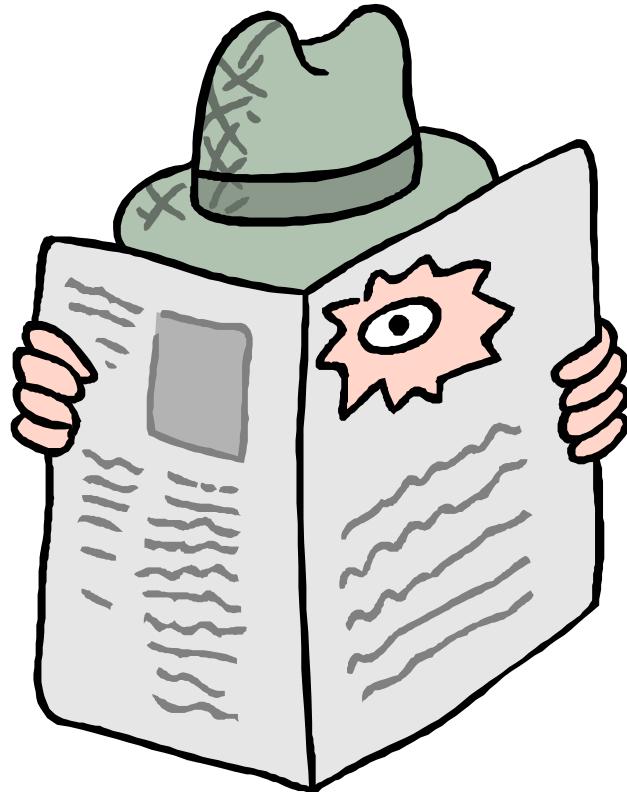


Sophos is available to Bowdoin students and employees for free



## 7. Use Anti-spyware Software

---



- ▶ Use anti-spyware software so unknown people cannot lurk on your computer and potentially steal your information
- ▶ Many anti-virus products include this feature (Sophos does)
- ▶ Spybot, Ad-Aware



“Free” software often contains hidden spyware – read user agreements carefully



## 8. Keep Your Computer Updated

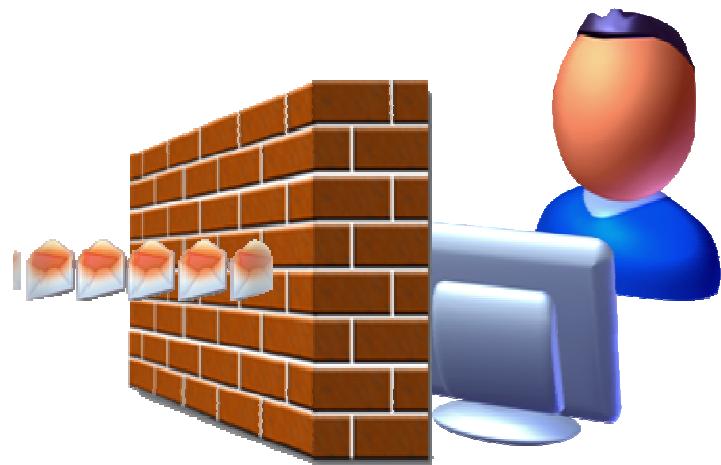
---

- ▶ 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



## 9. Use a Firewall

---



- ▶ An Internet firewall is like a moat around a castle, creating a barrier between your computer and the Internet
  
- ▶ Most popular operating systems have one built in
  - **Check to make sure it is on**



## 10. 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





Quiz

**From:** "TECHNICAL SUPPORT TEAM" <[infodesk@webmaster.edu](mailto:infodesk@webmaster.edu)>  
**Date:** December 15, 2008 1:07:47 PM GMT+09:00  
**To:** undisclosed recipient  
**Subject:** DEACTIVATION OF EMAIL ACCOUNT RESPOND ASAP.p  
**Reply-To:** [upgrade.centre@live.com](mailto:upgrade.centre@live.com)

Dear Account User,

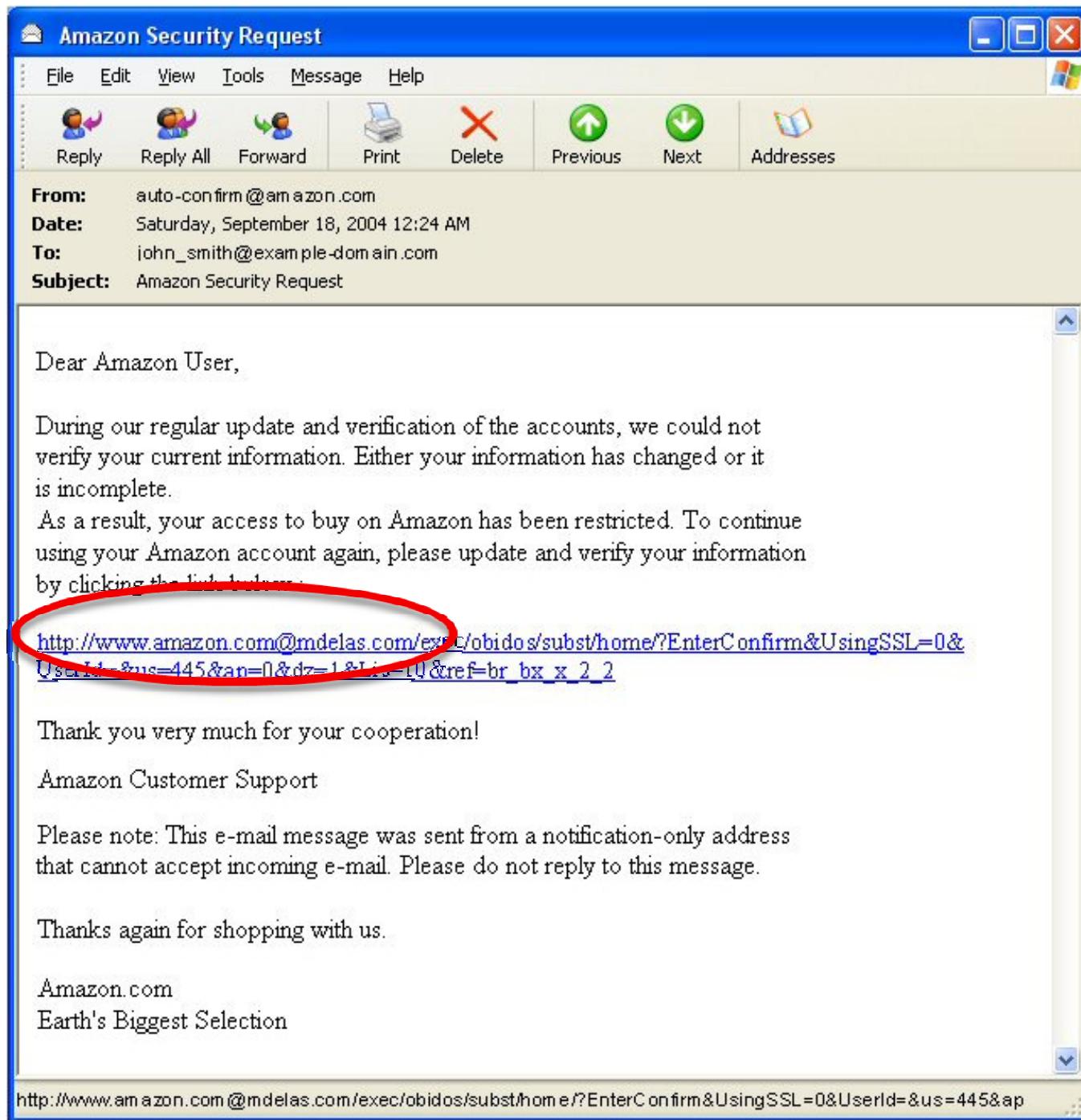
Important Notice - We have temporarily limited access to sensitive account features. To regain full account access, please you must reply to this email immediately and enter your E-mail account Username here: (.....)and password here:(.....)and

Due to the junk/spam emails you receive daily, we are currently upgrading all email accounts spam filter to limit all unsolicited emails for security reasons and to upgrade our new features and enhancements with your new and improved E-mail account, to ensure you do not experience service interruption.

Please you must reply to this email immediately and enter both your username and password in the space provided to enable us upgrades your Account.

A confirmation link will be send to you for the Re-Activation of you're-mail Account, as soon as we received your response and you are to Click on the "Confirm E-mail" link on your mail Account box and then enter this confirmation number: 1265-6778-8250-83

Kind regards,  
The webmail Service Technical Team.  
All rights reserved.



Suspicious activity in your account.

File Edit View Tools Message Help

Reply Reply All Forward Print Delete Previous Next Addresses

**From:** Washington Mutual  
**Date:** Tuesday, November 02, 2004 5:22 AM  
**To:** john@example-domain.com  
**Subject:** Suspicious activity in your account.

**Washington Mutual** AUTHORIZATIONS / CLEARING AND SETTLEMENT DEPARTMENT

Dear respected member of Washington Mutual Bank,

Our department recorded a payment request from Expedia - Online Travel Agency ( EXPEDIA.COM ) to enable the charge of \$619.49 on your account.

This amount is supposed to cover the cost of a 5 days reservation ( 06-11 November / 2004 ) at a Five Stars Hotel located in New Delhi / INDIA, under the name of GARY EDWARDS.

**THE PAYMENT IS PENDING FOR THE MOMENT.**

- If you made this reservation or if you just authorize this payment, please ignore or remove this email message. The transaction will be shown on your monthly statement as "Rama Bangalore-Hotel".
- If you didn't make this payment / reservation and would like to decline the \$619.49 billing to your card, please follow the link below to deny the payment:

**decline**

(Click "DECLINE" button to stop this payment.)

We apologize for any inconvenience this may cause, and appreciate your assistance in helping us maintain the integrity of the entire Washington Mutual, Inc. system.

Thank you for your prompt attention to this matter.

Please do not reply to this mail. Mail sent to this address cannot be answered

<http://dmswebsolutions.com/main/>

**Subject:**Your Account Expires In Seven (7) Days.

Date:Thu, 4 Dec 2008 00:05:14 +0100 (CEST)

**From:**BOWDOIN WEB USER <[info@bowdoin.edu](mailto:info@bowdoin.edu)>

**Reply-To:**[customer.care2008@hotmail.com](mailto:customer.care2008@hotmail.com)

To:undisclosed-recipients::

Dear BOWDOIN.EDU Web mail User,

This message was sent automatically by a program on BOWDOIN.EDU Web mail which Periodically checks the size of inbox, where new messages are received. The Program is run weekly to ensure no one's inbox grows too large. If your Inbox becomes too large; you will be unable to receive new email.

Just before this message was sent, you had 18 Megabytes (MB) or more of Messages stored in your inbox on BOWDOIN.EDU Web mail. To help us re-set your SPACE on our database prior to maintain our INBOX, you must reply to this

E-mail: [customer.care2008@hotmail.com](mailto:customer.care2008@hotmail.com) your Current

User name (            )

Password (            ).

You will continue to receive this warning message periodically if your Inbox size continues to be between 18 and 20 MB. If your inbox size Grows to 20 MB, then a program on BOWDOIN.EDU Web mail will move your oldest Email to a folder

in your home directory to ensure that you will continue to be able to receive incoming email. You will be notified by email that this has taken place.

If your inbox grows to 25 MB, you will be unable to receive new email as it will be returned to the sender.

After you read a message, it is best to REPLY and SAVE it to another Folder.

► Thank you for your cooperation. BOWDOIN.EDU Help Desk E-mail:  
[customer.care2008@hotmail.com](mailto:customer.care2008@hotmail.com)

What is the most important thing you can do to protect your computer?

---

- A. Turn on automatic updates
- B. Turn on the firewall
- C. Install anti-virus software and keep it updated
- D. Remove the hard drive
- E. A, C, and D
- F. A, B, and C
- G. A, B, C and D
- H. C and D



# Which is an example of a strong password?

---

- A. Password
- B. J\*p2le045>F
- C. Your real name or user name
- D. Your company name



If I have a network firewall, I don't need to use my host firewall.

---

A. True

B. False



Hackers are not interested in my computer.

---

A. True

B. False



# What personal information should you be careful about giving out?

---

- A. Hair color
- B. Social Security Number
- C. Phone number
- D. Credit Card Number
- E. Password for your investment account
- F. Name
- G. Date of Birth
- H. Drivers license number
- I. Mother's Maiden Name
- J. Your favorite pet's name



## What are the information security risks when I email?

---

- A. Email is always secure, there are no risks
  - B. My message may be read in transit
  - C. My message (and any attachments) may be forwarded to someone that I did not want to receive the message
  - D. My message may be changed and forwarded
  - E. My message may be changed in transit
- F. B, C, D and E are all email security risks





## Questions