

# Every Trick in the Book

Richard C. Pasco, Ph.D.

# Definitions

- **Virus:** That which tricks its host into making more copies of itself
- **Malware:** Malicious software
- **Trojan Horse:** Tricks users into installing hidden “features”
- **Spyware:** Like E.T., “phones home”

# Two kinds of Viruses

- Executable Software
- E-mail virus

# About Executable Files

- What does “open” mean?
- Executable files are everywhere
- Unsolicited executable files
- Virus scanners
- Identifying executable files

# Common Misconceptions

- “I have a virus scanner on my computer so I'm safe.”
- “I tried to open an attachment but lucky for me it failed”
- “If I had a virus here, it has not done anything.”
- “I did not have the suspicious message on the computer when I wrote others so, if was a virus, I didn't pass it on.”

# What about Macs?

- Macs need antivirus software
- Registry
- Root Access
- Java
- Flash, Quicktime, Adobe Reader
- Spyware is a web threat

# Protect Yourself

- Keep your software up-to-date.
- Don't open e-mail attachments.
- Don't follow instructions in unsolicited e-mail.
- Keep a good virus scanner running.
- Connect through a router/firewall.

# How to spot an e-mail virus

- Says "forward to everyone you know" or "this is really true" or similar.
- Has an urgent-sounding warning, a heart-wrenching plea, an offer of something for nothing, or a heart-warming story.
- Has technical-sounding language with details glossed over.
- Gives no reference to contact the original author for more information (phone number, e-mail address, etc.)
- Seeks credibility by naming known institutions, publications, etc., but lacks details (contact persons, publication dates, web pages).
- Uses terms like "yesterday" or "this week" in an un-dated message.
- Promises you good luck if you forward it, or threatens bad luck if you don't.

# Hacked or Spoofed?

- **Hacked:** Mail sent from your account by someone logged in to your server as you.
- **Spoofed:** Mail sent from elsewhere with your address forged onto its "From:" line.

# Evidence of Hacked e-mail

- **Full Name** on “From:” line
- Your **address book** used
- **Launching Server**
- **Copy** saved in “Sent Mail” folder

# How did they get my password?

- They guessed it
- They obtained it from your service provider
- You gave it to them
- You used the same password elsewhere
- Spyware in your computer

***Never* give your e-mail  
password to anyone  
or enter it into any web site**

other than your own e-mail server  
in the normal course of logging in  
to read your mail.

# Fixing a Hacked E-mail Account

- Will changing my password fix everything?
- Should I change my e-mail address?
- Close out old, unused e-mail accounts

# Spoofed: Your address forged onto the "From:" line

- Keep your e-mail address private
- Keep your contact's addresses private

# E-mail Tricks

- The “software update” trick
- The “notification pending” trick
- The “order confirmation” trick
- The parcel delivery problem
- The travel reservations trick
- “Is this you in this video?”
- “I liked your profile ... here's mine”

# More E-mail Tricks

- The “job offer” scam
- The erotic photo trick
- “Your e-mail account will be terminated”
- The “Credit Card Overdue” trick
- The “Better Business Bureau” trick

**Subject:** ALERT !

**From:** "XFINITY"<online.communications@alerts.comcast.net>

**Date:** 1/6/2012 8:43 PM



Dear Comcast Customer,

Our records show that we unable to process your most recent payment. Did you recently change your bank, phone number or credit card?.

---

**To ensure that your service is not interrupted, please update your billing information by clicking [Update Your Account Information](#).**

---

We're available 24 hours a day, 7 days a week. Please don't hesitate to contact us.

If you have recently updated your billing information, please disregard this message as we are processing the changes you have made.

Sincerely,

Comcast Member Services Team

P.S. Comcast has several pricing options to meet your needs.

PLEASE DO NOT REPLY TO THIS E-MAIL. THIS E-MAIL ADDRESS IS USED BY: COMCAST AUTOMATED SYSTEMS AND IS NOT MONITORED.

**1-800-COMCAST**  
[www.comcast.com](http://www.comcast.com)

# For More Information

- Web: <http://www.richpasco.org/virus/>

- E-mail:

<http://www.richpasco.org/cgi-bin/contact.cgi>