

Email

Be Cyber Savvy with C-SAFE

Fact:

More computers are attacked when users open email attachments than by *all other vectors combined*

Two primary attack vectors:

Attachments

HTML (*Hypertext Markup Language*)

94

Email Attachments

Message Labs claims that 1 in every 60 emails contains malware

- Malicious software: you launch the payload when you double-click it
- Anti-virus software protects you... IF you have set it to scan your email
- Malware is generally (but not always) in the form of *executable* files (.exe .vbs .com .bat .scr)

95

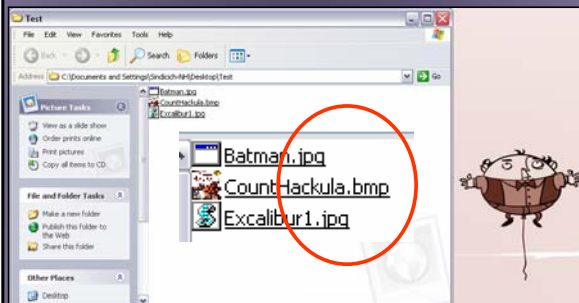
Does avoiding executable files save me?

Sorry...but no!

- Other types of files can also contain malware
- Plus you can't trust the file based on what you *think* the extension is
 - Files extensions are easy to fake
 - Sometimes (Windows) computers are configured to hide the REAL extension

96

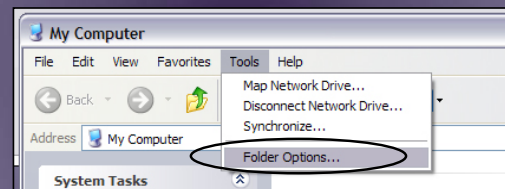
Hidden File Extensions



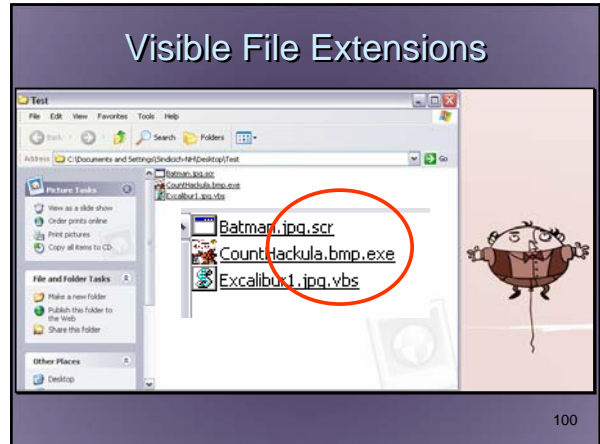
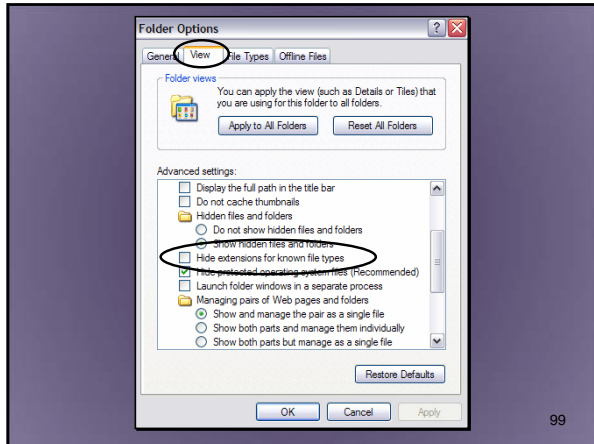
97

How to display extensions

My computer>>Tools>>Folder Options



98



Fact:

Reading the email message, or *simply viewing it in a preview screen*, could immediately activate any hidden malicious content

It can:

- Install malware on your computer
- Validate your email address

HTML vs. Plain Text Email

HTML

Plain Text

Review all email in Plain Text

HTML code can hide malicious software

Fix:

- Use *plain text only* to review your email
- Try Pocketknife Peek
www.xintercept.com/pkpeek.htm

Apply the VEKS test before you view any email

The VEKS Test

Consider deleting emails that do not pass:

- The *Virus Test*
– Does the email contain a virus
- The *Expect Test*
– Were you expecting an attachment from this sender
- The *Know Test*
– Is the email from someone you know
- The *Sense Test*
– Does the subject make sense or is it full of gibberish

Spam

Be Cyber Savvy with C-SAFE

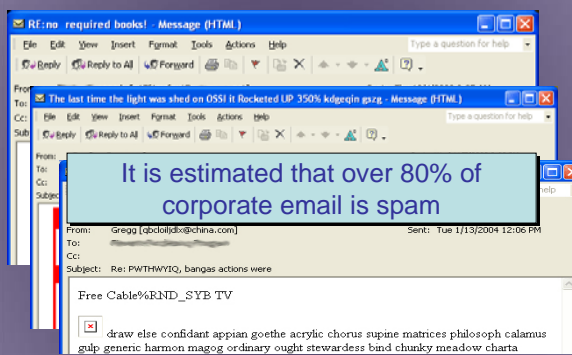
Spam

Unsolicited Commercial Email (UCE)

Unsolicited: you didn't ask for it
Commercial: it wants your money

Not to be confused with "Not Spam" or Unintentionally solicited email

107



It is estimated that over 80% of corporate email is spam

108

How can I tell where it's coming from?

Sometimes you can but...

- Bullet proof hosts

Normally you can't...

- Use of one-time email accounts
- Spoofing

109

Spoofing

Forging mail headers to make it appear that messages originated elsewhere

Often used by spammers and scammers

110

How do spammers get my email address?

- Buying mailing lists from third parties
- Adding people to opt-in lists
- "Bots" scouring the Internet (universities, businesses, forums)
- "Brute forcing" popular domains (aol.com, yahoo.com, comcast.net)

111

The CAN SPAM Act of 2003

- Overrides ALL state anti-spam laws
- Prohibits spoofing the email address of the sender
- Forbids the harvesting of email addresses from websites
- Requires a “working” opt-out link

So why isn't the CAN SPAM Act working?

112

The CAN SPAM Act of 2003

Also mentioned:

- Do Not Spam List
- Reporting/reward mechanism

Controlling the Assault of Non Solicited Pornography and Marketing

113

Tips for Fighting Spam

- Don't open it! Don't open it! Don't open it!
- Never click on the “opt-out” link
- Don't reply to spam
- Never buy anything advertised in spam
- Screen the spam from the not-spam
- Post a “throw-away” email address on websites and newsgroups (hotmail, yahoo, gmail, dodgeit)

114

More Tips for Fighting Spam

- Disguise your email address (you@yahoo.com = you at yahoo dot com)
- Check the privacy policy before giving your email address
- Use the “Report Spam” feature of your email client
- Consider spam filters

115