

IT Security

An Introduction (DARC)

Matthew Cook
<http://escarpment.net/>

Agenda

- Why Bother?
- Terminology
- Physical Security
- Password Security
- Viruses
- Worms
- Trojans
- Phishing
- SPAM
- Spy/Ad Ware
- P2P Networks
- Encryption
- Operating System Patching
- Incident Response
- Not just Computers
- Windows Security
- Linux Security
- Wireless Security

Why bother?

Why bother?

- Keeping control and service availability
- Spreading infection
- Data Integrity (DPA)
- Legal Liability
- Reactive Work Loads
- Bad Public Relations
- Personal Responsibility

Why bother?

- Computing has changed...
- Ten years ago the Internet was very small, few connections, mainly dialup users.
- JANET connected UK Universities from the early 90s.
- ISDN links at 64Kb/sec for industry.
- Advent of broadband brings many, many more users on a fast connection.

Why bother?

- Personal Attacks
- Information theft and modification
- Experimentation
- Bandwidth theft
- DoS Botnets
- Warez servers
- Distribute Viruses, Worms and Trojans

Terminology

- Compromised – Is the technically correct term for ‘hacked’. (Slang: owned)
- Cracker – Someone who breaks into computer systems for malicious reasons.
- Hacker – Someone who is creative with computers.
- Script Kiddie – Someone who runs security related scripts without much knowledge of the technology, usually teenagers.

Terminology...

- Virus – Malicious code.
- Worm – Code spread automatically, usually via the Internet.
- Trojan – A piece of computer code hidden on a system to usually gain back door access.
- Bandwidth – The amount of data that can flow along a computer link.
- DoS Attack – Denial of Service attack.

Terminology...

- IP Address – A unique address on a network specific to one machine (similar to a phone number).
- Port – A specified number between 1 and 65535 through which data can be exchanged with computer programs.
- Root – The super user account on the computer usually Root on Unix/Linux or Administrator on Windows.

Physical Security

"The only system which is truly secure is one which is switched off and unplugged, locked in a titanium lined safe, buried in a concrete bunker, and is surrounded by nerve gas and very highly paid armed guards. Even then, I wouldn't stake my life on it."

Gene Spafford

Physical Security...

- Secure Location
- BIOS restrictions
- Password Protection
- Boot Devices
- Case Locks
- Case Panels

Password Security

The object when choosing a password is to make it as difficult as possible for a cracker to make educated guesses about your chosen password. This leaves them no alternative but a brute-force search, trying every possible combination of letters, numbers, and punctuation.

Password Security...

- Do not use your login name in any form
- Do not use your first or last name
- Do not use your spouse's or child's name
- Do not use your Car Registration etc.
- Do not use a dictionary based password
- Do not use a password shorter than 8 chars
- Do not write it on 'post-it' notes

Password Security...

- Use a password with mixed-case characters
- Use a password with a mix of alphanumeric and punctuation
- Use a password that is easy to type to avoid 'Shoulder Surfers'
- Use the first letters from song titles, song lyrics or film quotations

Viruses

- Traditional viruses required human intervention.
 - Share it on floppy discs
 - Copy it
 - Email it
- Attached to programs, documents or emails.

Worms

- One stage on from viruses
- Auto replication
 - Open shares
 - Exploits in machines
 - Outlook Address book
- Eliminating the human interaction means whole computer networks can be compromised very swiftly.

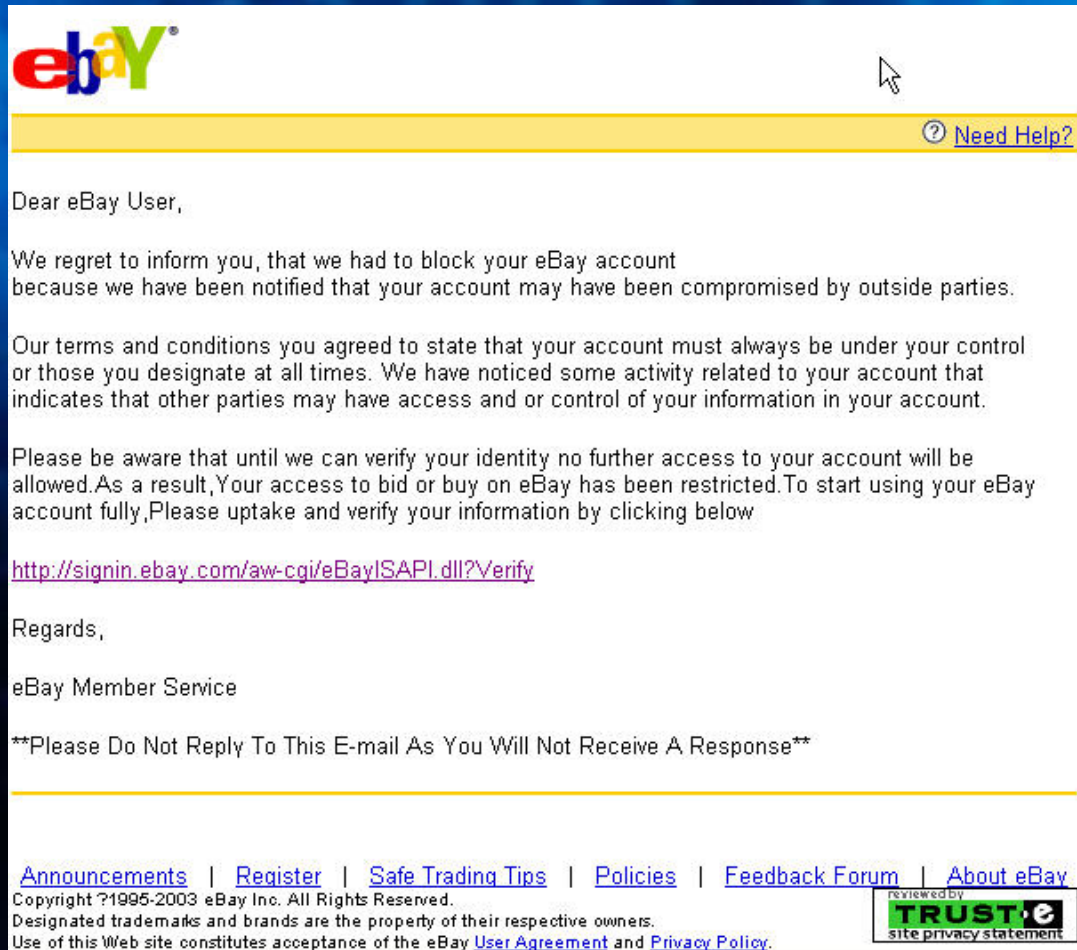
Trojans

- Appears to be an innocent program
- Actually contains malicious code
- Quite often a backdoor to the system
- Sometimes difficult to discover


Phishing

- The term given to the attempted theft of information by misleading information.
- Your Bank account has been compromised, please give us your account details...
- Your Email account has been suspended, please give us your password...
- Very common: Banks, eBay, PayPal etc

Phishing...



The screenshot shows a phishing email designed to look like an official eBay communication. It features the eBay logo in the top left corner and a yellow navigation bar with a "Need Help?" link. The body of the email contains a message from "eBay Member Service" stating that the recipient's account has been blocked due to suspected compromise. It includes a link to a verification page and a warning not to reply to the email. At the bottom, there are links to various eBay pages and a "TRUSTe" privacy statement logo.

 [? Need Help?](#)

Dear eBay User,

We regret to inform you, that we had to block your eBay account because we have been notified that your account may have been compromised by outside parties.

Our terms and conditions you agreed to state that your account must always be under your control or those you designate at all times. We have noticed some activity related to your account that indicates that other parties may have access and or control of your information in your account.

Please be aware that until we can verify your identity no further access to your account will be allowed. As a result, Your access to bid or buy on eBay has been restricted. To start using your eBay account fully, Please uptake and verify your information by clicking below


<http://signin.ebay.com/aw-cgi/eBayISAPI.dll?Verify>

Regards,

eBay Member Service

****Please Do Not Reply To This E-mail As You Will Not Receive A Response****

[Announcements](#) | [Register](#) | [Safe Trading Tips](#) | [Policies](#) | [Feedback Forum](#) | [About eBay](#)
Copyright ?1995-2003 eBay Inc. All Rights Reserved.
Designated trademarks and brands are the property of their respective owners.
Use of this Web site constitutes acceptance of the eBay [User Agreement](#) and [Privacy Policy](#).



Phishing...

Sign In

New to eBay? or **Already an eBay user?**

If you want to sign in, you'll need to register first.

Registration is fast and **free**.

[Register >](#)

eBay members, sign in to save time for bidding, selling, and other activities.

eBay User ID

[Forgot your User ID?](#)

Password

[Forgot your password?](#)

[Sign In >](#)

[Keep me signed in](#) on this computer unless I sign out.

[Account protection tips](#) | [Secure sign in \(SSL\)](#)

You can also register or sign in using the following service:

[Announcements](#) | [Register](#) | [Security Center](#) | [Policies](#) | [Feedback Forum](#) | [About eBay](#)

Copyright ©1995-2004 eBay Inc. All Rights Reserved.
Designated trademarks and brands are the property of their respective owners.
Use of this Web site constitutes acceptance of the eBay [User Agreement](#) and [Privacy Policy](#).

reviewed by
TRUST
site privacy statement

Phishing...

ebay
Security Update [help](#)

For security reasons the following information must be confirmed.

Your eBay ID and Password - Your email address used as your login for your eBay account and your eBay password.

User ID: ← The bogus ID accepted by the phisher

Email address:

Alternative password - In order to prevent any fraudulent activity from occurring we strongly advise you to specify an alternative eBay password. This process allows us to give back sole control of the account to you in case something goes wrong with instructions regarding the account and its future safety.

Alternative password:

Account Security Section - For security purposes, please enter the following security questions accordingly.

Mother's Maiden Name:

Date Of Birth:

Driver License Number:

State of Issue:

Social Security Numbers:

Your Profile Information - Your name and address as you have it listed for your credit card or bank account.

First Name:

Last Name:

Address 1:

Address 2:

(optional)

City:

State:

State / Province / Region:

Zip Code:

Country:

Home Telephone:

Work Telephone:

(optional)

Your Credit Card Information - Your credit card used with your eBay account.

Card Type:

Credit Card Number:

Expiration Date:

CV Code:

Card PIN Code:

Card Issuing Bank:

Your Bank Account Information - Your bank account used with your eBay account.

Bank Name:

Account Type:

Routing Number:

Account Number:

Retype Account Number:

[Announcements](#) | [Register](#) | [Security Center](#) | [Policies](#) | [Feedback Forum](#) | [About eBay](#)

Copyright 1995-2004 eBay Inc. All Rights Reserved.
Designated trademarks and brands are the property of their respective owners.
Use of this Web site constitutes acceptance of the eBay [User Agreement](#) and [Privacy Policy](#).

Phishing...



Thank You For Your Update [help](#)

You have successfully updated your Account information.

[Click here to login.](#)

[Announcements](#) | [Register](#) | [Security Center](#) | [Policies](#) | [Feedback Forum](#) | [About eBay](#)

Copyright ?1995-2004 eBay Inc. All Rights Reserved.


Designated trademarks and brands are the property of their respective owners.

Use of this Web site constitutes acceptance of the eBay [User Agreement](#) and [Privacy Policy](#).



Phishing...

Microsoft All Products | Support | Search | Microsoft.com Guide
Microsoft Home

 Microsoft Customer

this is the latest version of security update, the "June 2004, Cumulative Patch" update which fixes all known security vulnerabilities affecting MS Internet Explorer, MS Outlook and MS Outlook Express as well as three newly discovered vulnerabilities. Install now to continue keeping your computer secure from these vulnerabilities. This update includes the functionality of all previously released patches.

System requirements	Windows 95/98/Me/2000/NT/XP
This update applies to	MS Internet Explorer, version 4.01 and later MS Outlook, version 8.00 and later MS Outlook Express, version 4.01 and later
Recommendation	Customers should install the patch at the earliest opportunity.
How to install	Run attached file. Choose Yes on displayed dialog box.
How to use	You don't need to do anything after installing this item.

Microsoft Product Support Services and Knowledge Base articles can be found on the [Microsoft Technical Support](#) web site. For security-related information about Microsoft products, please visit the [Microsoft Security Advisor](#) web site, or [Contact Us](#).

Thank you for using Microsoft products.

Please do not reply to this message. It was sent from an unmonitored e-mail address and we are unable to respond to any replies.

The names of the actual companies and products mentioned herein are the trademarks of their respective owners.

Contact Us | Legal | TRUSTe
©2004 Microsoft Corporation. All rights reserved. [Terms of Use](#) | [Privacy Statement](#) | [Accessibility](#)

SPAM

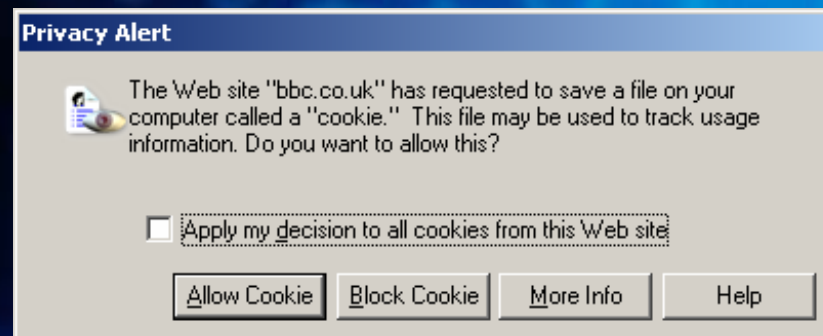
- Unsolicited email or advertising messages.
- Selling pharmaceuticals, pornography, web site links, make money fast schemes, chain letters, fraud etc
- Clogs up mailboxes and wastes space and bandwidth.
- Currently filtered out on our email routers.

Spy/Ad Ware

- Vulnerabilities with Operating Systems and browsers allow the tracking of your web browsing, information gathering and the display of advertising information.
- Check cookies.
- Use only trusted software.
- Be careful what you download or run.
- - Project to start to look at these issues.

Spy/Ad Ware

- Selectively accept cookies in Internet Explorer
 - Tools -> Internet Options -> Privacy -> Advanced.



P2P Networks

- Common source of Trojan files
 - Appealing for free downloads
 - Most are illegal and copyrighted material
 - Against most ISPs Acceptable Use Policy
- Source of excessive bandwidth

Firewalls

- Block access to malicious traffic entering the network.
- Block outgoing traffic which may have malicious affects.
- Bi-directional: Protects us from the rest of the world and protects the rest of the world from us.
- Different types of policies; default deny and default allow.

Firewalls...

- Personal Firewalls are not recommended as the only line of defence or an excuse not to patch.
- Software Firewalls often fail open.
- Hardware Firewalls traditionally fail closed.
- Most broadband routers contain firewall features (including NAT).

Encryption...

- In the early days of computing messages were sent in clear text across the wire.
- People using 'packet sniffers' could read these messages, including passwords and steal the identity of a user.
- Encryption methods are now used to prevent this happening.
- Examples; SSH, HTTPS, VPNs...

Operating System Patching...

- Operating Systems do contain bugs, and patches are a common method of distributing these fixes.
- A patch or hot fix usually contains a fix for one discovered bug.
- Service packs contain multiple patches or hotfixes. There are well over 200 hot fixes in most service packs.

Operating System Patching...

- Its not just the Operating System!
 - Software needs patching too
 - Lots of vulnerabilities are discovered in software.
 - MS Office, GDI+ JPEG Module, IIS, MS SQL, Oracle etc

Incident Response...

- Don't Panic!
- Unplug the network
- Don't turn the computer off.
- Get a notebook
- Back-up the system and keep the Back-ups
- Look for information
- Investigate the cause

- Request help and assistance.

Incident Response...

- Important to return to service swiftly
 - Do not jeopardize security
 - Always, re-build
 - Perform forensics on a backup
- Keep documentation and evidence

Not just Computers

- Network appliances
- Printers
- Photocopiers
- CD towers
- Network switches, routers, firewalls
- Anything network connected...

Windows Security

- Automatic Updates
 - My Computer > Select Properties > Select Automatic Updates tab.
 - We do NOT recommend Automatic or Turning Automatic Updates off.
 - Either; Download updates for me, but let me choose when to install them.
 - OR Notify me but don't automatically download or install them.

Windows Security...

- Microsoft Baseline Security Analyser
- Freely available from Microsoft
- Provides advice on
 - Security best practices
 - Strong passwords
 - Security mis-configurations
 - Application configurations

Linux Security

- Choose a sensible partitioning structure
- Install only the required packages
- Remove Unnecessary services
 - Nmap
 - Chkconfig
 - Restart
- Update via YUM

War Driving

- Kismet
- Detects insecure wireless networks
- Provides SSID
- Can map networks with a GPS unit
- Free wireless networks available...

Securing Wireless

- Configure the network and clients
- Use a suitable encryption method
- Use MAC address filtering/locking
- Do not broadcast SSID
- Further security
 - Offer limited or no DHCP scope
 - Check Logs

Further Information

- Vendor Sites
- <http://escarpment.net/>
- <http://www.lboro.ac.uk/computing/security/>
 - Advice and Guidance
 - Training
 - Links

Security Notifications

2004 - 2005	IT-Security	Windows-Security	Unix-Security	Mac-Security
September	5	1	0	0
October	2	8	1	3
November	2	5	1	2
December	4	4	3	3
January	3	5	0	2
February	12	12	18	7
March	18	4	26	3
April	11	4	45	3
Total	57	43	94	23
Grand total	217			41

Questions and Answers

<http://escarpment.net/>