Unit I

Introduction: Malwares

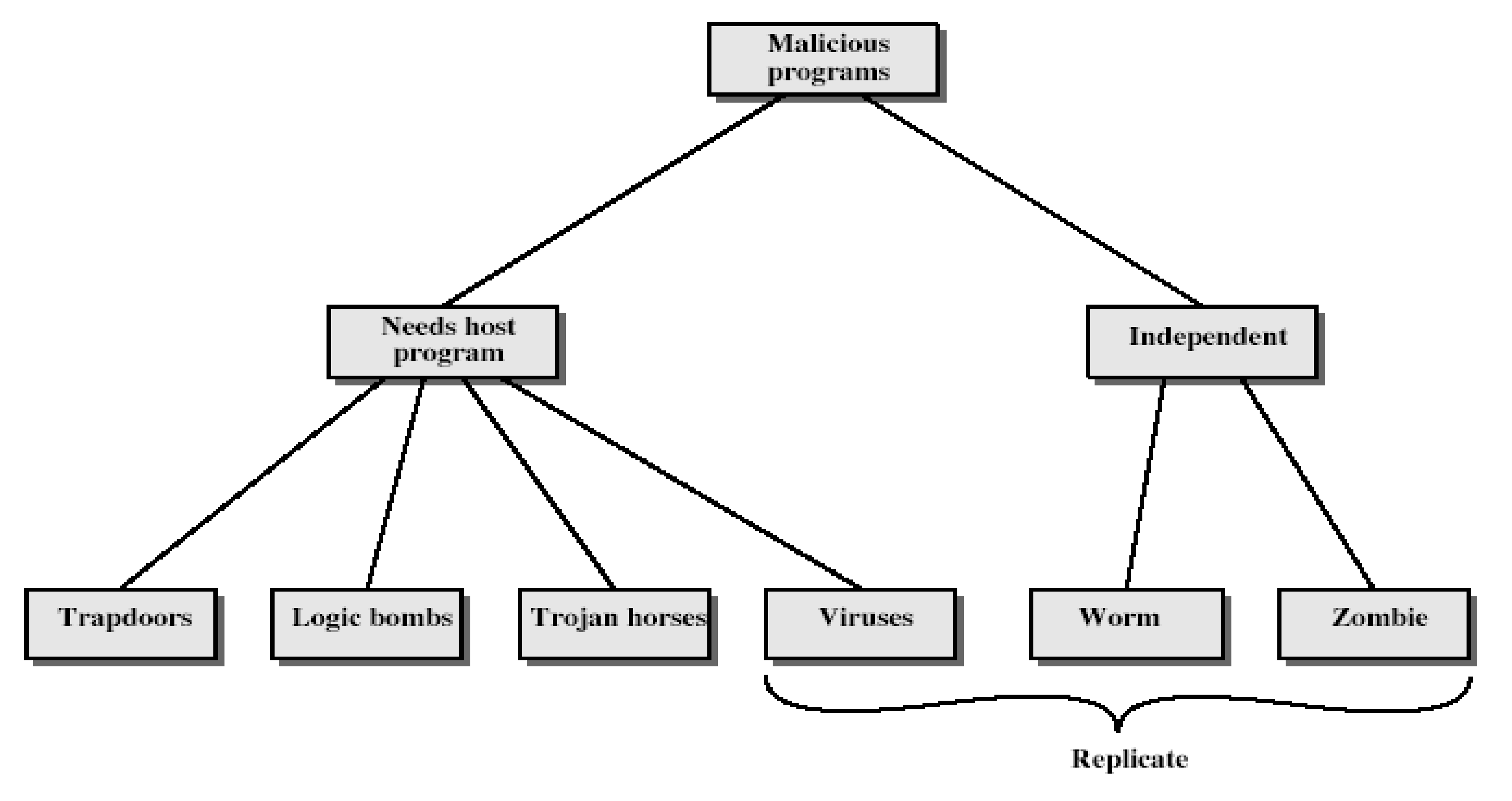
Attack

- Any action that compromises the security of information owned by an organization
- information security is about how to prevent attacks, or failing that, to detect attacks on information-based systems
- have a wide range of attacks
- can focus of generic types of attacks
- note: often *threat* & *attack* mean same

Classify Security Attacks as

- **Passive attacks** - eavesdropping on, or monitoring of, transmissions to:
  - – obtain message contents, or
  - – monitor traffic flows
- **Active attacks** – modification of data stream to:
  - – masquerade of one entity as some other
  - – replay previous messages
  - – modify messages in transit
  - – denial of service

Malicious Software



Viruses

- A **virus** is a small piece of software that piggybacks on real programs in order to get executed
- Once it’s running, it spreads by inserting copies of itself into other executable code or documents
- Propagates itself & carries a payload
  - carries code to make copies of itself
  - as well as code to perform some covert task

Virus Operation

- virus phases:
  - dormant – waiting on trigger event
  - propagation – replicating to programs/disks
  - triggering – by event to execute payload
  - execution – of payload
- details usually machine/OS specific
  - exploiting features/weaknesses

Virus Structure

```
program V :=
    {goto main;
    1234567;
    subroutine infect-executable :=   {loop:
                     file := get-random-executable-file;
                     if (first-line-of-file = 1234567) then goto loop
                     else prepend V to file; }
    subroutine do-damage :=           {whatever damage is to be done}
    subroutine trigger-pulled :=      {return true if some condition holds}
    main: main-program := {infect-executable;
                                      if trigger-pulled then do-damage;
                                      goto next;}
    next:
}
```

Types of Viruses

Can classify on basis of how they attack

- parasitic virus
- memory-resident virus
- boot sector virus
- Stealth virus
- polymorphic virus
- Micro virus

Macro Virus

- **macro code** attached to some **data file**
- interpreted by program using file
  - eg Word/Excel macros
  - esp. using auto command & command macros
- code is now platform independent
- is a major source of new viral infections
- blurs distinction between data and program files making task of detection much harder
- classic trade-off: "ease of use" vs "security"

Email Virus

- spread using email with attachment containing a macro virus
  - e.g. Melissa
- triggered when user opens attachment
- or worse even when mail viewed by using scripting features in mail agent
- usually targeted at Microsoft Outlook mail agent & Word/Excel documents

Logic Bomb

- one of oldest types of malicious software
- code embedded in legitimate program
- activated when specified conditions met
  - e.g. presence/absence of some file
  - particular date/time
  - particular user
- when triggered typically damage system
  - modify/delete files/disks

Zombie

- program which secretly takes over another networked computer
- then uses it to indirectly launch attacks
- often used to launch distributed denial of service (DDoS) attacks
- exploits known flaws in network systems

Worms

A **worm** is a small piece of software that uses computer networks and security holes to replicate itself.

- A copy of the worm scans the network for another machine that has a specific security hole.
- It copies itself to the new machine and starts replicating from there

Worms

- replicating but not infecting program
- typically spreads over a network
  - e.g. Morris Internet Worm in 1988
  - led to creation of CERTs
- using users distributed privileges or by exploiting system vulnerabilities
- widely used by hackers to create **zombie PC's**, subsequently used for further attacks, esp DoS
- major issue is lack of security of permanently connected systems, esp PC's

Worm Operation

- worm phases like those of viruses:
  - dormant
  - propagation
    - search for other systems to infect
    - establish connection to target remote system
    - replicate self onto remote system
  - triggering
  - execution

Recent Worm Attacks

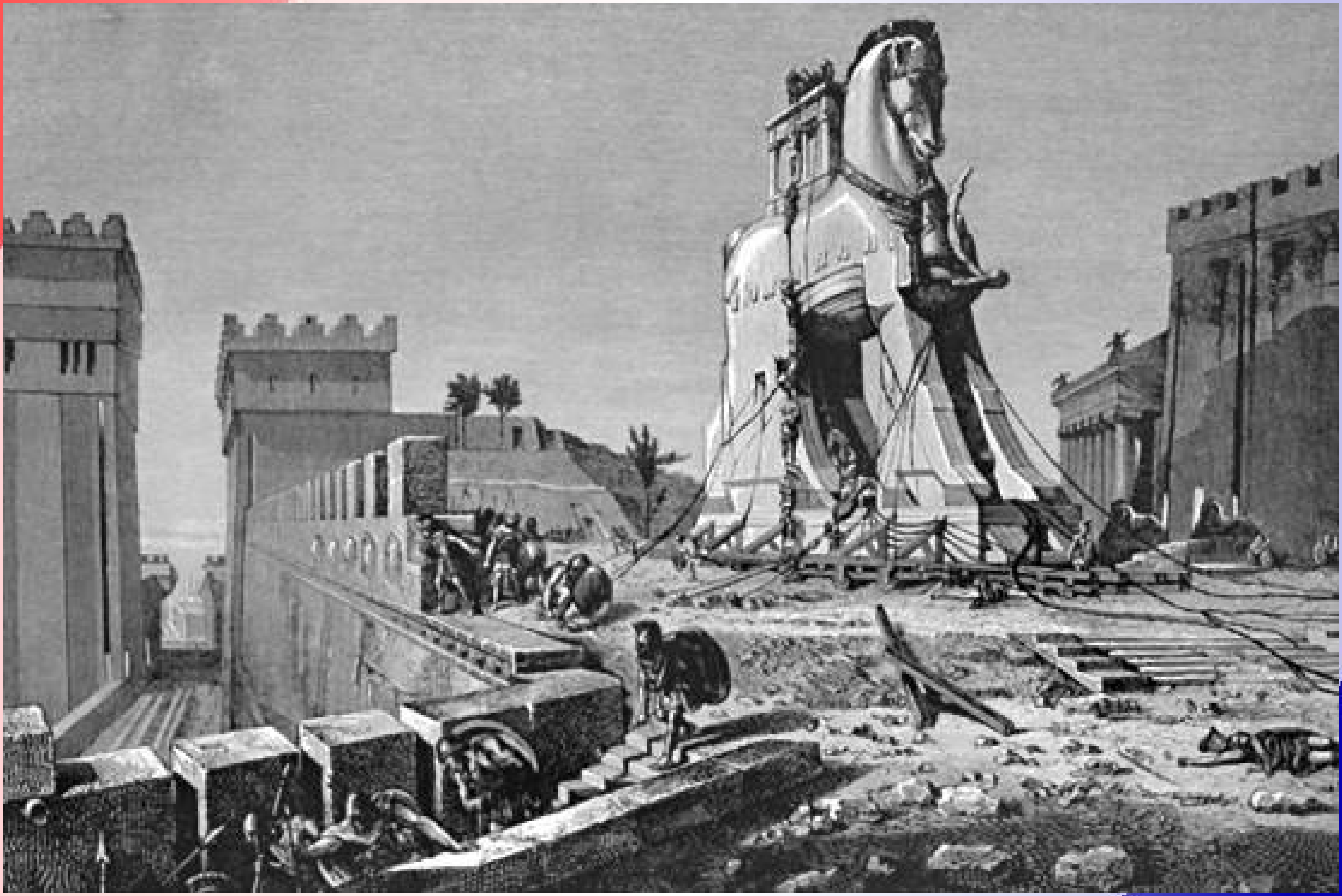
- new kind of attacks from mid-2001
- **Code Red**
  - exploited bug in MS IIS to penetrate & spread
  - probes random IPs for systems running IIS
  - had trigger time for denial-of-service attack
  - 2nd wave infected 360000 servers in 14 hours
- **Code Red 2**
  - had backdoor installed to allow remote control
- **Nimda**
  - used multiple infection mechanisms
    - email, shares, web client, IIS, Code Red 2 backdoor

Morris Worm

- best known classic example of worm
- released by Robert Morris in 1988
- targeted Unix systems
- using several propagation techniques
  - simple password cracking of local pwd file
  - exploit bug in finger daemon
  - exploit debug trapdoor in sendmail daemon
- if any attack succeeds then replicated self

Trojan horse

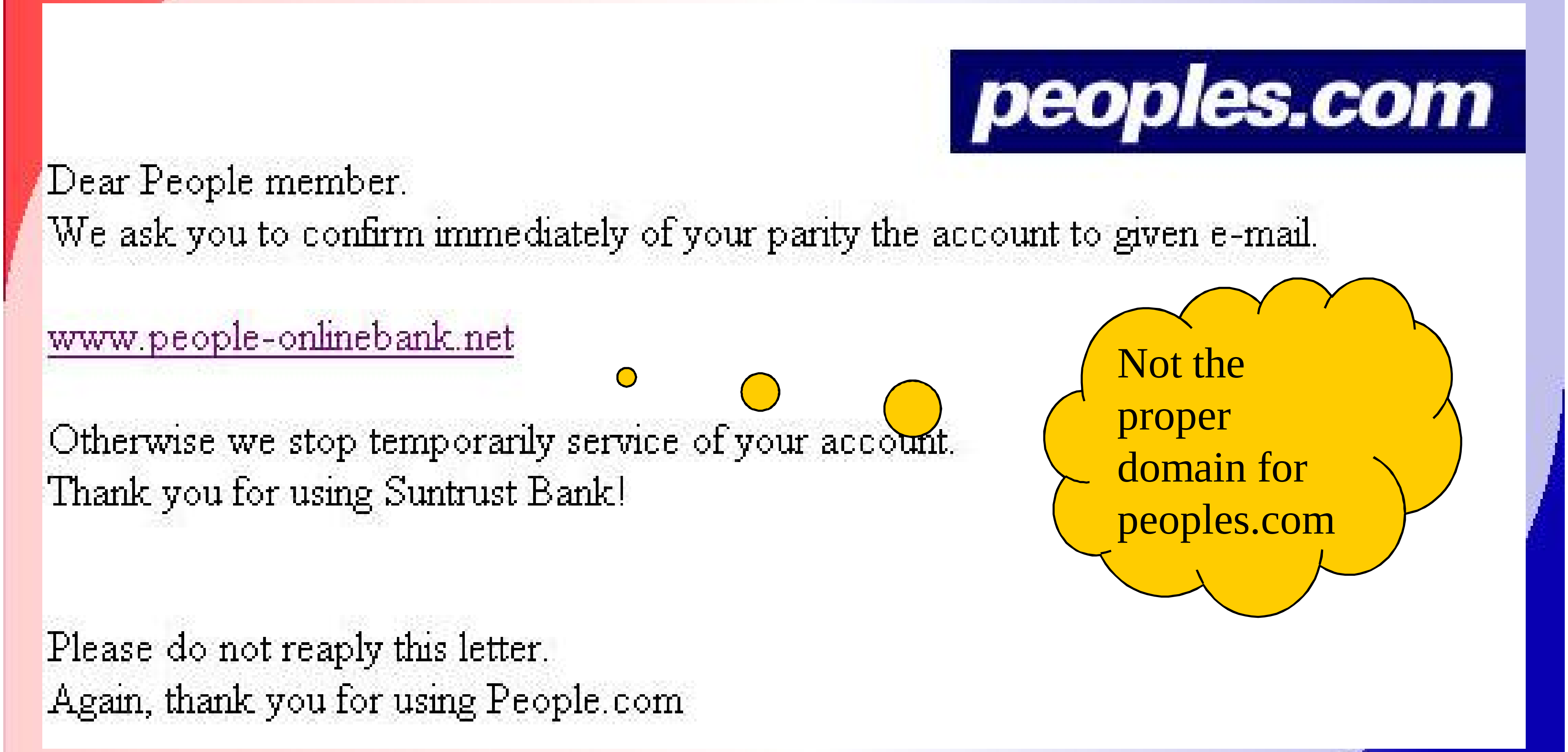
- The term comes from Greek mythology about Trojan War.
- A computer program that appears to perform one function while actually doing something else, such as inserting a virus into a computer system or stealing a password.



Phishing

- The typical phishing attack involves a fraudulent email message sent to thousands of users. On reading such emails, few users respond by revealing their bank account information to the hackers

People’s Bank



peoples.com

Dear People member.
We ask you to confirm immediately of your parity the account to given e-mail.

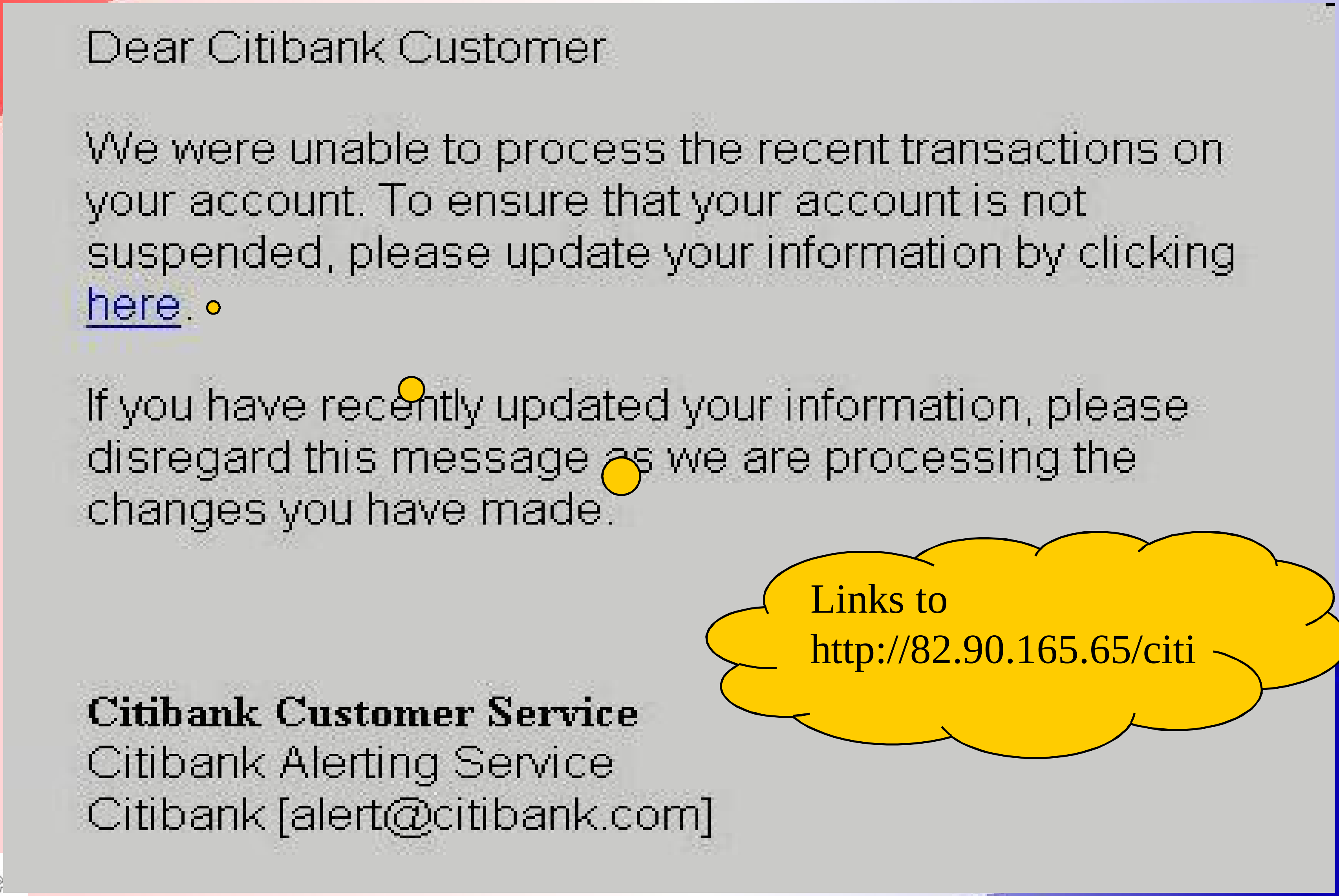
www.people-onlinebank.net

Otherwise we stop temporarily service of your account.
Thank you for using Suntrust Bank!

Please do not reaply this letter.
Again, thank you for using People.com

Not the proper domain for peoples.com

Citibank (Nov 10)



Dear Citibank Customer

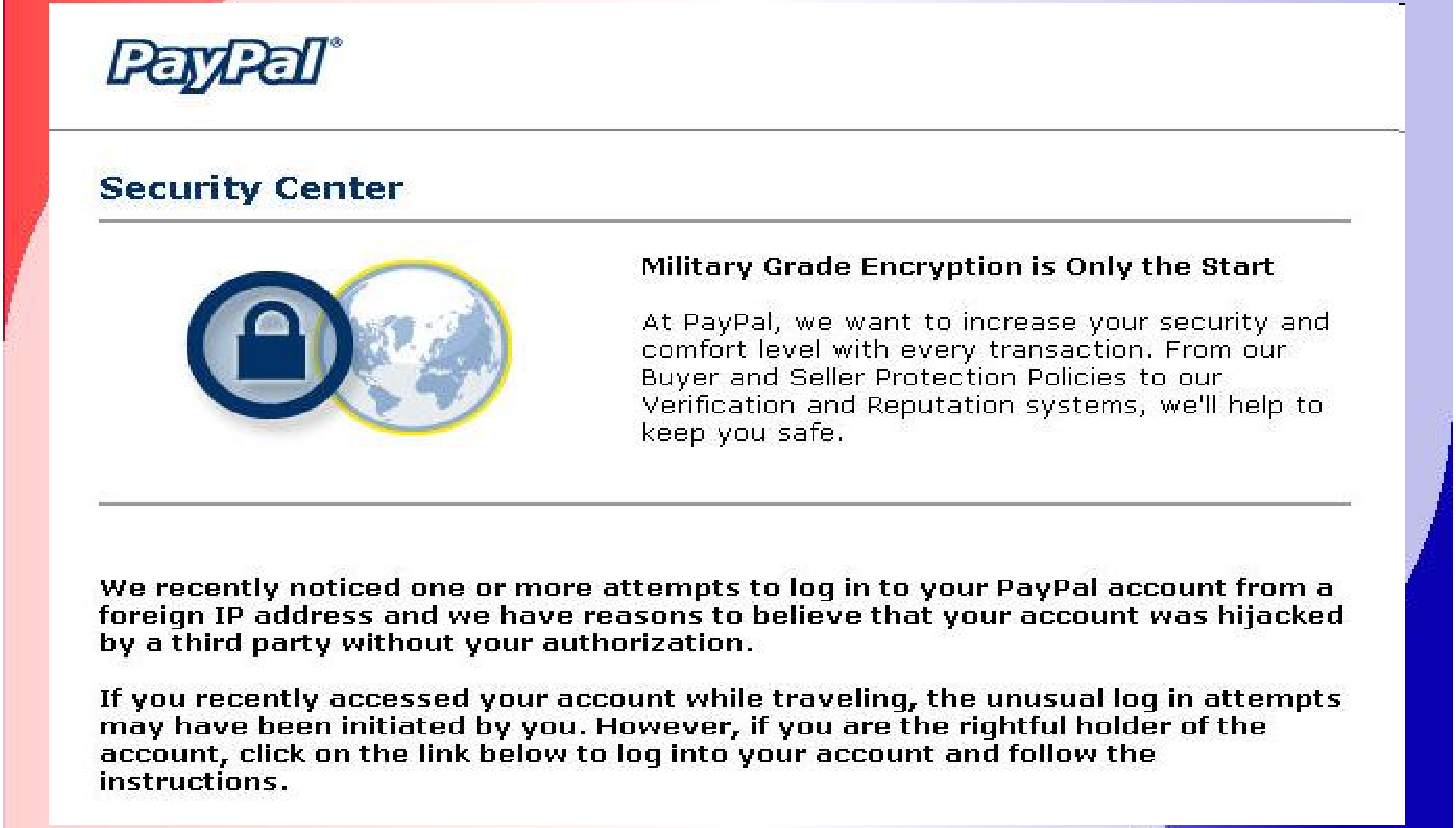
We were unable to process the recent transactions on your account. To ensure that your account is not suspended, please update your information by clicking here.

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

Citibank Customer Service
Citibank Alerting Service
Citibank [alert@citibank.com]

Links to
http://82.90.165.65/citi

PayPal (1)



Security Center

Military Grade Encryption is Only the Start

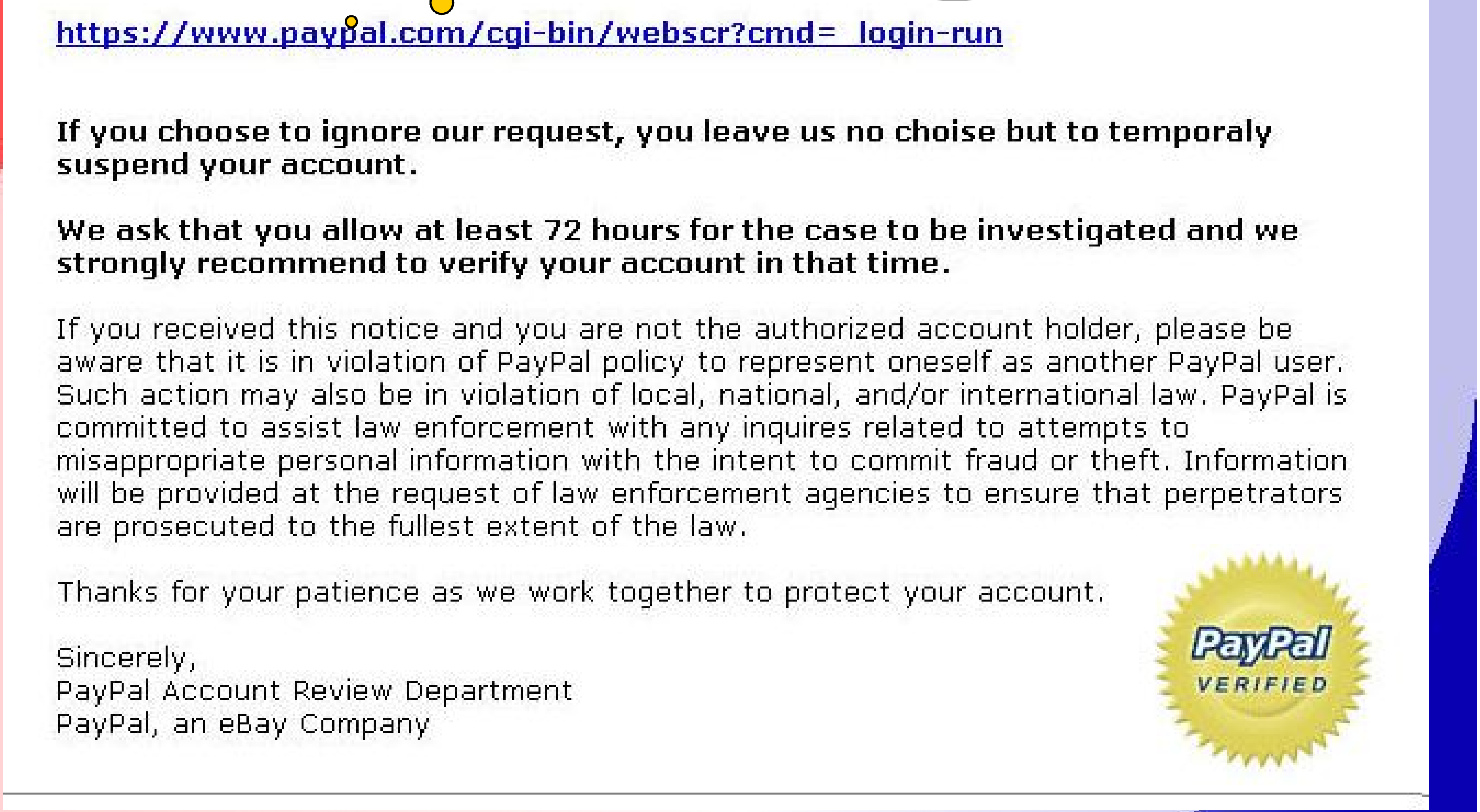
At PayPal, we want to increase your security and comfort level with every transaction. From our Buyer and Seller Protection Policies to our Verification and Reputation systems, we'll help to keep you safe.

We recently noticed one or more attempts to log in to your PayPal account from a foreign IP address and we have reasons to believe that your account was hijacked by a third party without your authorization.

If you recently accessed your account while traveling, the unusual log in attempts may have been initiated by you. However, if you are the rightful holder of the account, click on the link below to log into your account and follow the instructions.

PayPal (2)

Actually links to http://212.45.13.185/.paypal/index.php



https://www.paypal.com/cgi-bin/webscr?cmd=_login-run

If you choose to ignore our request, you leave us no choise but to temporaly suspend your account.

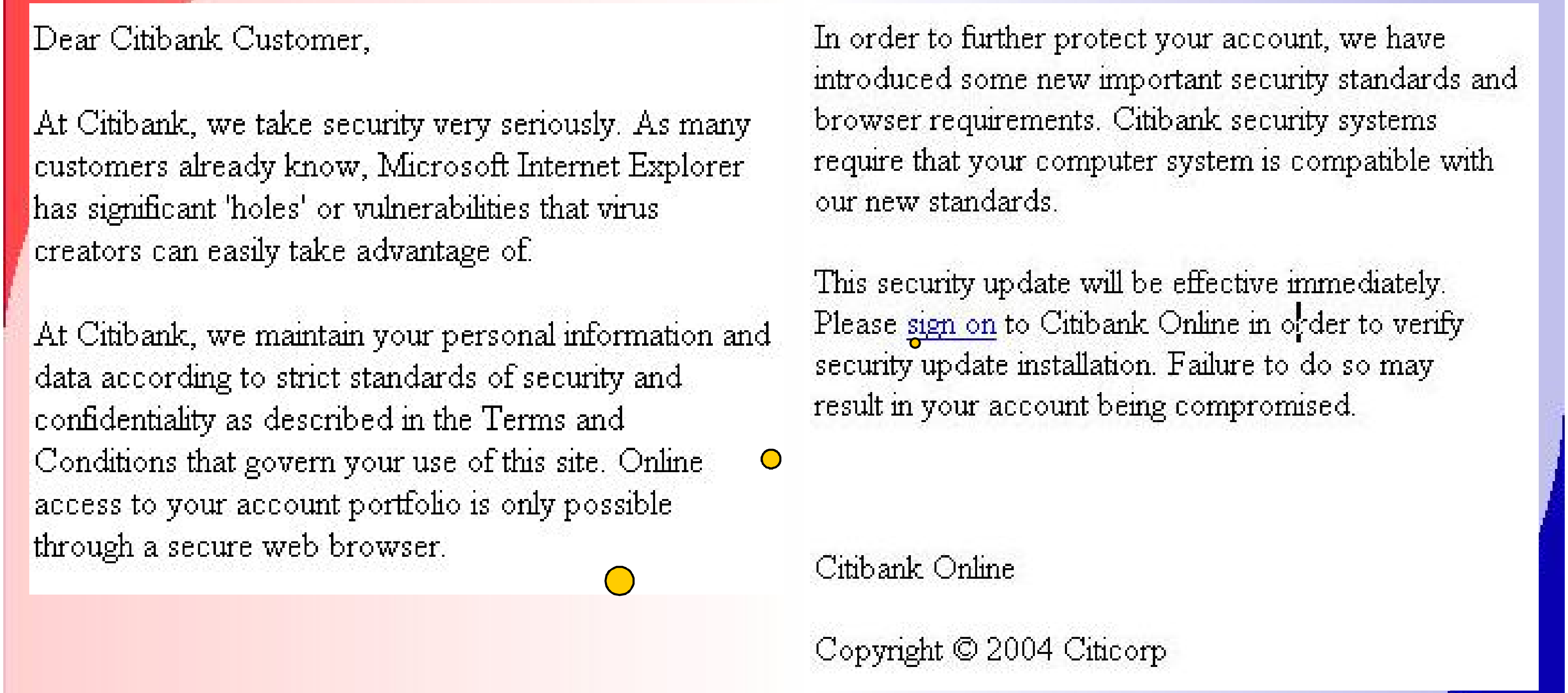
We ask that you allow at least 72 hours for the case to be investigated and we strongly recommend to verify your account in that time.

If you received this notice and you are not the authorized account holder, please be aware that it is in violation of PayPal policy to represent oneself as another PayPal user. Such action may also be in violation of local, national, and/or international law. PayPal is committed to assist law enforcement with any inquires related to attempts to misappropriate personal information with the intent to commit fraud or theft. Information will be provided at the request of law enforcement agencies to ensure that perpetrators are prosecuted to the fullest extent of the law.

Thanks for your patience as we work together to protect your account.

Sincerely,
PayPal Account Review Department
PayPal, an eBay Company

Citibank (Nov 1)



Dear Citibank Customer,

At Citibank, we take security very seriously. As many customers already know, Microsoft Internet Explorer has significant 'holes' or vulnerabilities that virus creators can easily take advantage of.

At Citibank, we maintain your personal information and data according to strict standards of security and confidentiality as described in the Terms and Conditions that govern your use of this site. Online access to your account portfolio is only possible through a secure web browser.

In order to further protect your account, we have introduced some new important security standards and browser requirements. Citibank security systems require that your computer system is compatible with our new standards.

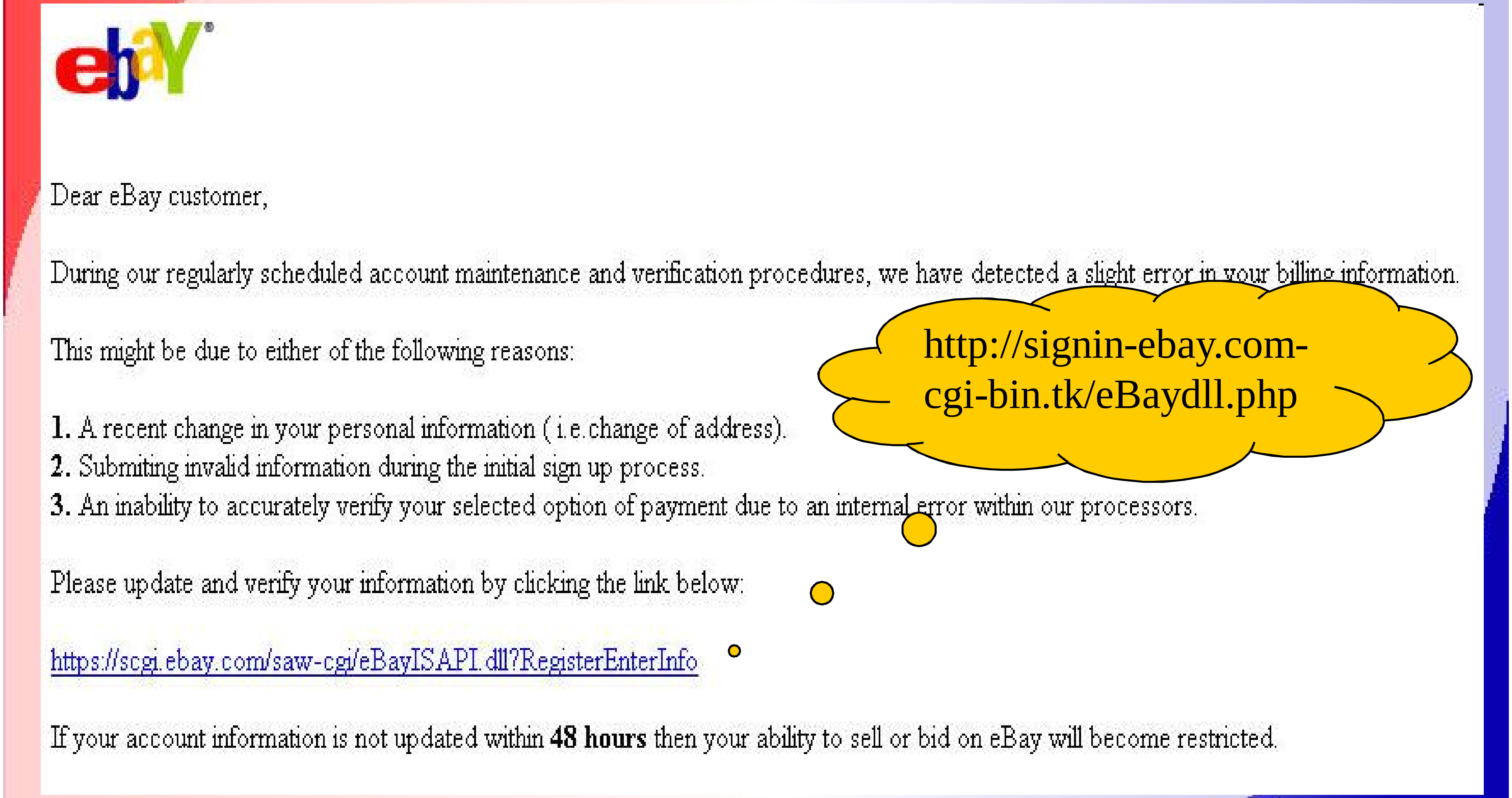
This security update will be effective immediately. Please sign on to Citibank Online in order to verify security update installation. Failure to do so may result in your account being compromised.

Citibank Online

Copyright © 2004 Citicorp

Links to http://200.189.70.90/citi/

eBay



Dear eBay customer,

During our regularly scheduled account maintenance and verification procedures, we have detected a slight error in your billing information.

This might be due to either of the following reasons:

1. A recent change in your personal information (i.e.change of address).
2. Submiting invalid information during the initial sign up process.
3. An inability to accurately verify your selected option of payment due to an internal error within our processors.

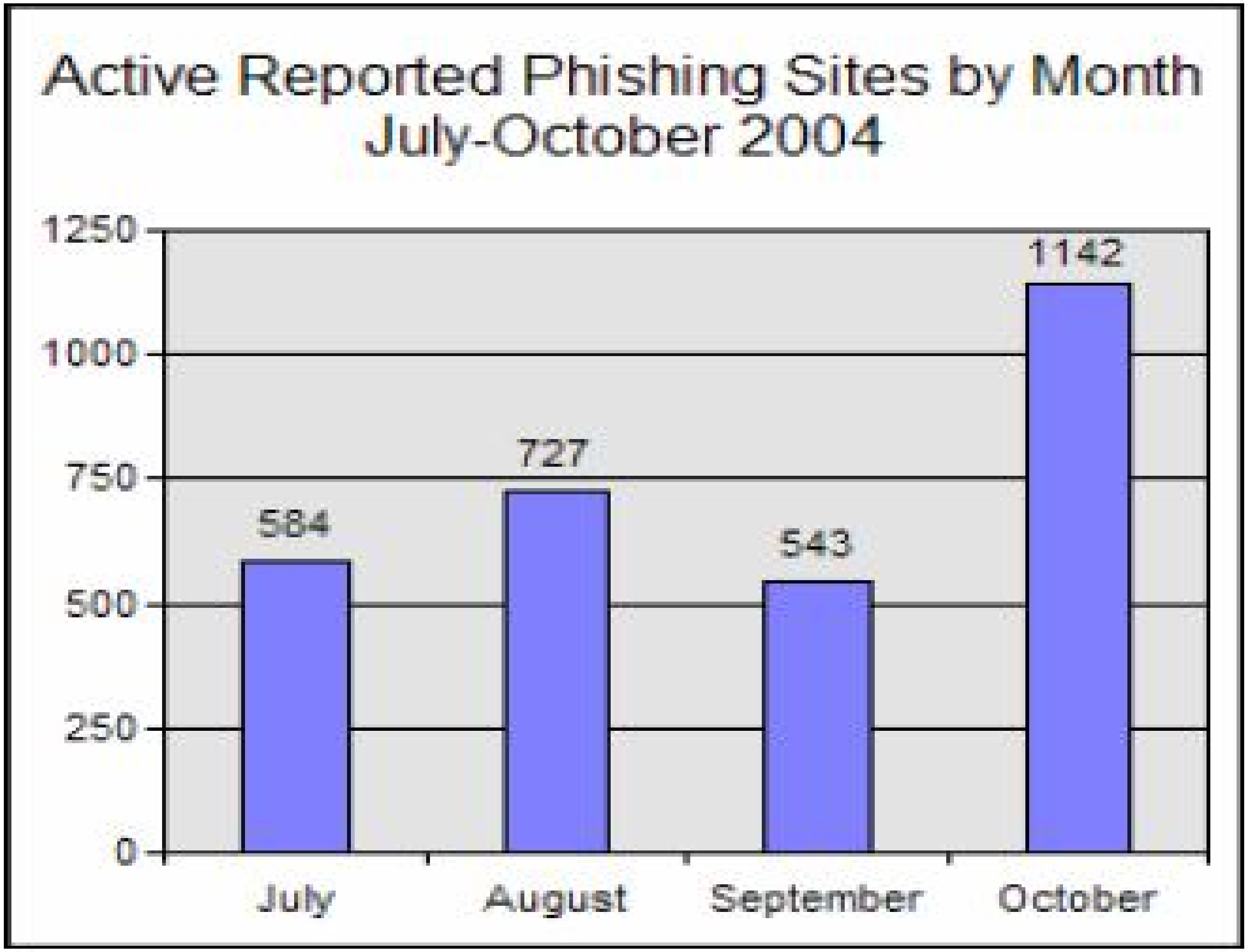
Please update and verify your information by clicking the link below:

https://scgi.ebay.com/saw-cgi/eBayISAPI.dll?RegisterEnterInfo

If your account information is not updated within **48 hours** then your ability to sell or bid on eBay will become restricted.

http://signin-ebay.com-cgi-bin.tk/eBaydll.php

Problem Increasing

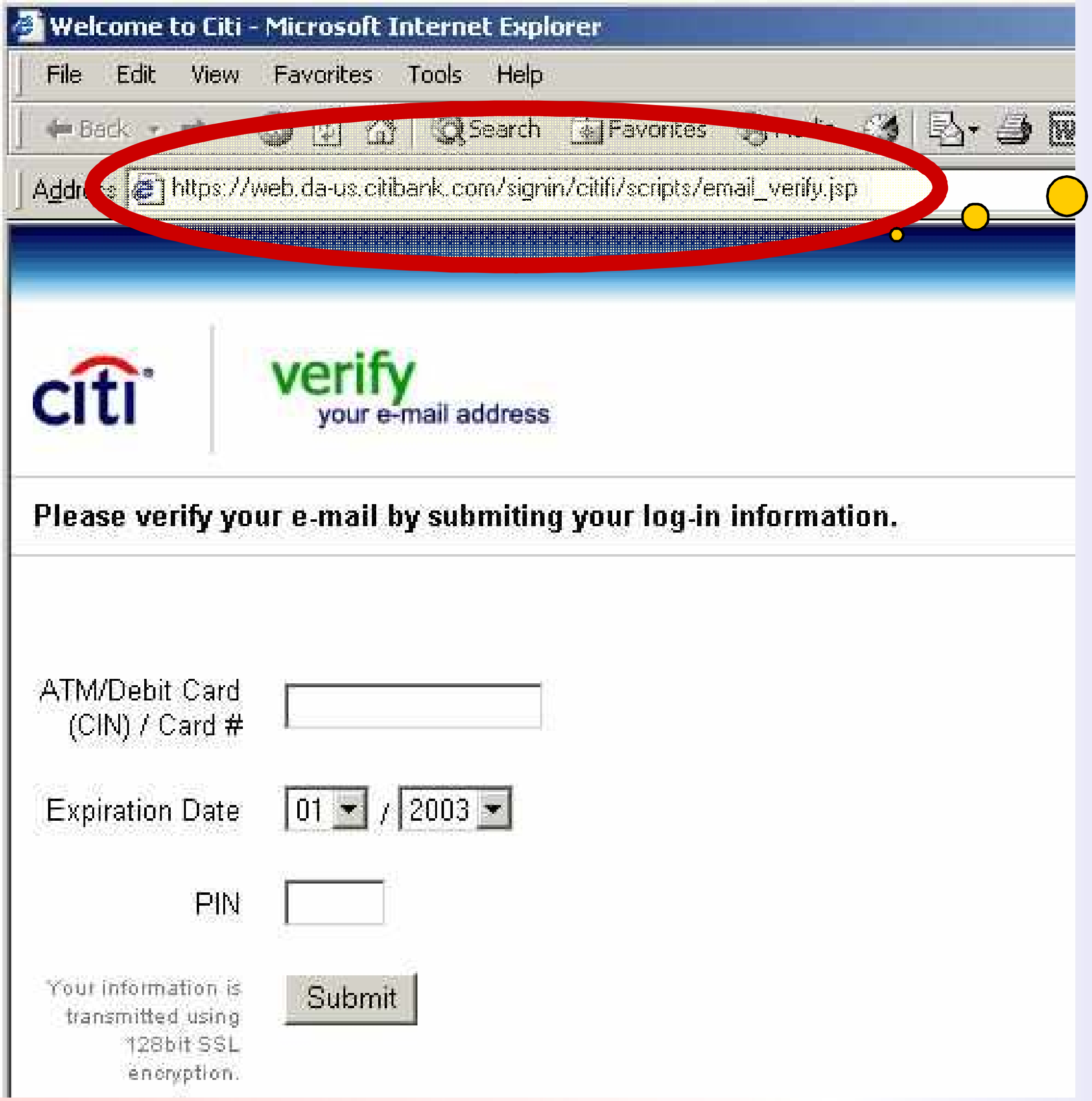


Anti-Phishing Working Group
http://www.antiphishing.org • info@antiphishing.org

Get a Job – and Lose Money

- Free training offer is latest spam scam
  - By John Leyden
  - Published Tuesday 2nd November 2004 12:35 GMT
  - http://www.theregister.com/2004/11/02/training_spam_scam/
- Apply for “training” and “job” at Credit Suisse
- Fill in banking details (!)
- Lose control over your financial information to criminals

Spoofed Page and Address Bar



Welcome to Citi - Microsoft Internet Explorer

Address https://web.da-us.citibank.com/signin/citifi/scripts/email_verify.jsp

verify your e-mail address

Please verify your e-mail by submiting your log-in information.

ATM/Debit Card (CIN) / Card #	
Expiration Date	01 / 2003
PIN	
Your information is transmitted using 128bit SSL encryption.	Submit

Not the real address bar

Spyware

- Spyware is program that is put in someone's computer to secretly gather information about the user and relay it to advertisers or other interested parties.

- Preventing spyware from getting onto your computer is your first step!
  - Do not download unnecessary software from the internet, especially free ones because they most likely have adware or spyware inside them.
  - If a download screen appears, asking you to confirm your download, click no if you not trying to install anything.
  - Avoid clicking advertised popups especially ones that mention “free” stuff if possible.

Recommendations

- Some adware/spyware files like to hide in the temporary internet folders.
- Disable saving of temporary files by going to Program Files, Control Panel, Network and Internet Connections, Internet Options, Temporary Internet Files Settings, Check Never under "Check for Newer Version of Stored Pages".
- Constantly delete old temporary files and cookies by going to Program Files, Control Panel, Network and Internet Connections, Internet Options, Delete Cookies and Delete Temporary Files.
- Remember though, adware and spyware can be tricky, no matter how cautious you are, there are bound to be adware or spyware programs that install into your computer.
  - Always constantly scan your computer for adware and spyware and keep your Adware/Spyware killer programs fully updated at all times.

How to prevent them

- Run a secure operating system like UNIX/LINUX or Windows NT
  - security features keep viruses away
- Buy virus protection software
- Avoid programs from unknown sources (like the Internet)
- Stick with commercial software purchased on CDs