



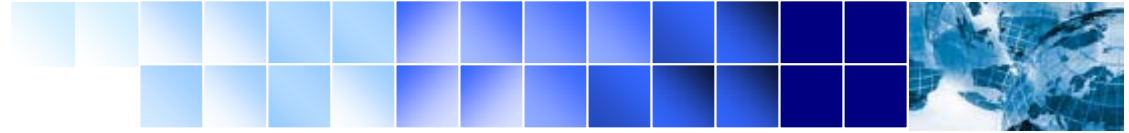
*National Computer Board*

# Anti-Spam End User Guidelines

**Reza Soodin**  
Research Officer, NCB  
[rsoodin@ncb.mu](mailto:rsoodin@ncb.mu)



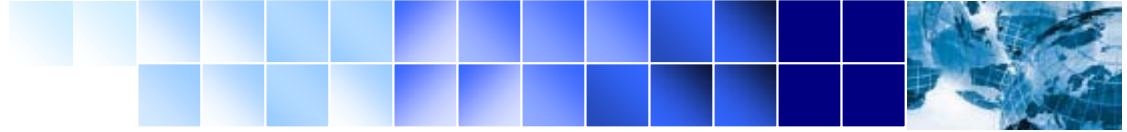
**19<sup>th</sup> February 2007**



---

# Agenda

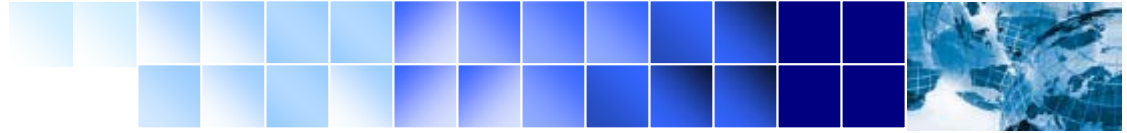
- ▶ Tips for sending/responding to emails
- ▶ Spam Associated Threats
- ▶ Lottery – Social engineering
  - **Phishing**
- ▶ Sophistications of attacks
- ▶ Conclusion



# Unknown/Unsolicited contacts

---





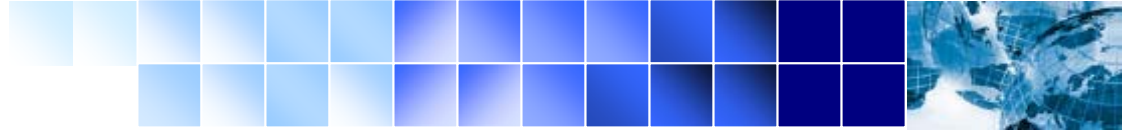
## Using Email

---

- ▶ **Ensure you are addressing the right person prior to sending email**
- ▶ **Beware of emails from unknown parties (unsolicited emails)**
- ▶ **Do not open unsolicited emails**
- ▶ **Do not click on links in unsolicited emails**
- ▶ **Never respond to unsolicited emails e.g. *‘You have won \$1,000,000. Kindly send your bank details for crediting your account.’* These are scams also known as social engineering attacks**

**Nigerian Scam**

**Foreign Lotteries**

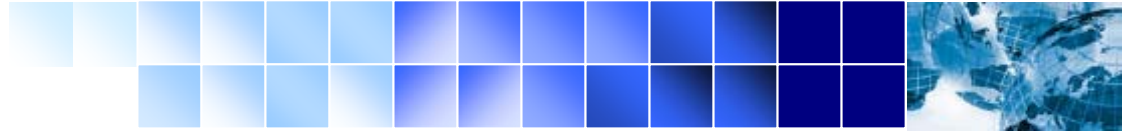


# Using Email

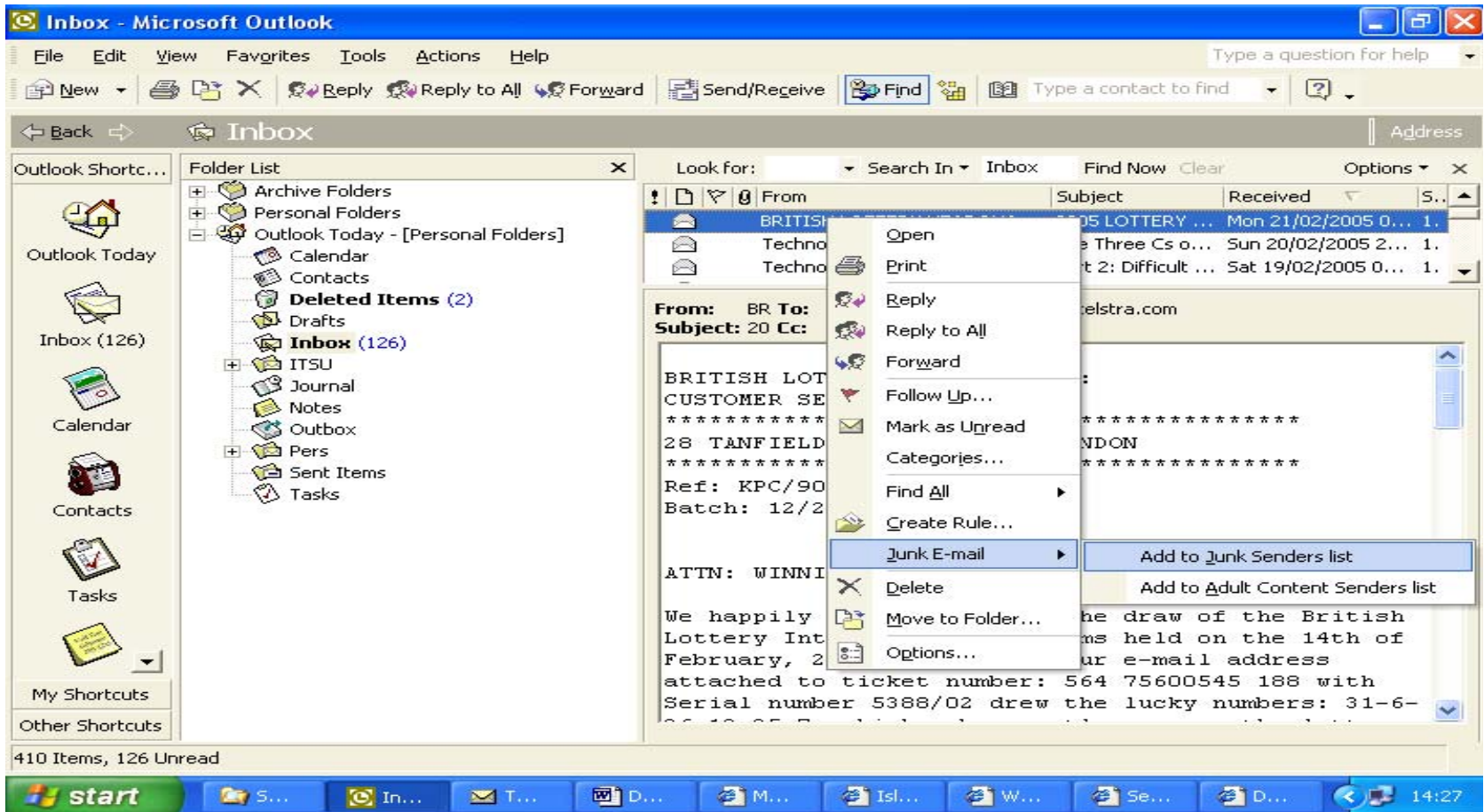
---

## Precautions

- ▶ **Suspicious attachments must NOT be opened**  
e.g. Executable files (with .exe, .com, .bat, .reg extensions)
- ▶ **Regularly purge unnecessary emails (including emptying the ‘Deleted Items’ or ‘Trash Can’ folder) to free storage space**
- ▶ **Do not open/reply to spam messages**
- ▶ **Avoid registering unnecessarily to mailing lists**
- ▶ **Use properly configured & regularly updated spam filter, antivirus and antispyware software**
- ▶ **Use firewall as well**



# Filtering Junk Mails

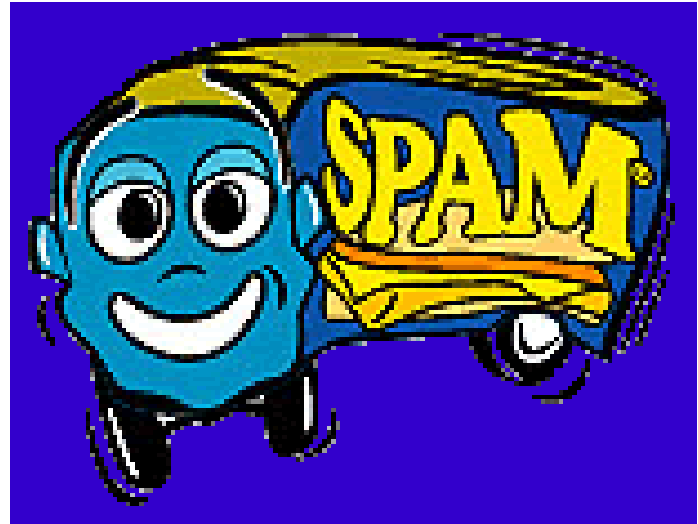


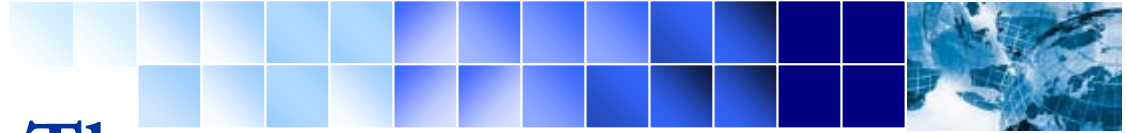
# Spam Associated Threats

---

Spam provides a cover for the spreading of:

- ▶ Viruses
- ▶ Worms
- ▶ Trojans
- ▶ Spyware
- ▶ Phishing





# Spam Associated Threats

---

- ▶ **Viruses**

Programs that can be attached to emails and are spread as files from individual to individual. Viruses are intentionally destructive

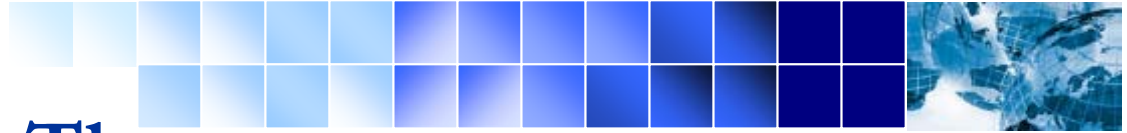
- ▶ **Worms**

Self replicating computers programs, similar to computer viruses however do not require other programs or documents to spread.

- ▶ **Trojans**

non-replicating malicious programs which appears harmless or even useful to the user but when executed harms the user's system

e.g of a trojan horse – “Waterfall.scr”



# Spam Associated Threats

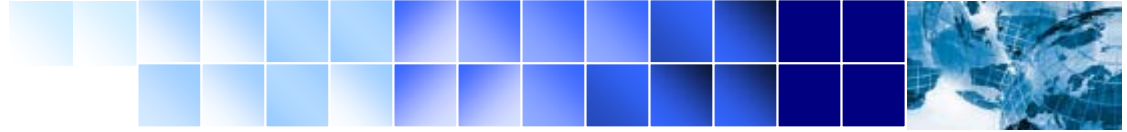
---

- ▶ **Spyware**

Programs installed on computers which record and send your personal information – includes marketing info( visited sites, lists of your software, your interests ,etc...)

- ▶ **Phishing**

attempt to fraudulently acquire sensitive information, such as password and financial information, through email or an instant message



# Solutions

---

## ▶ Spam Filters

- mail client filters (not adequate)
  - MS Outlook, Outlook Express...
- ISP filters (not adequate)

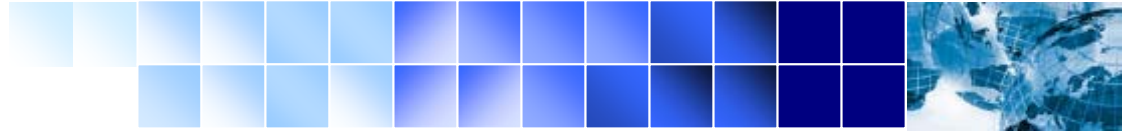
## ▶ Antivirus

AVG, Symantec, McAfee, F-Secure....

## ▶ Antispyware

McAfee Antispyware module, S&D , Ad-Aware  
SE personal....





# Lottery – Social Engineering

## AWARD FINAL NOTIFICATION:

We happily announce to you the draw (#999) of the UK NATIONAL LOTTERY,online Sweepstakes International program held on the 16th of January 2006. You were entered as dependent clients with: Reference SERIAL NUMBER: 144-66584 and Batch number BT-4478474121P.

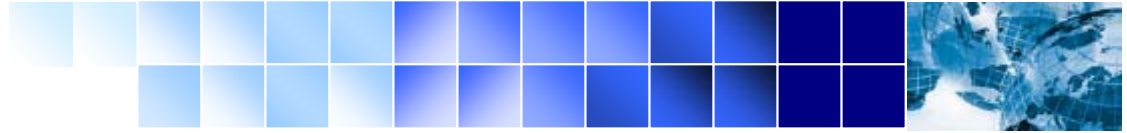
Your email address attached to the ticket number: 74454774 that drew the lucky winner



Bonus Ball [38]  
bonus. You ha  
£800,000.00 |  
file

Yours faithfully,  
Ms.Shelley Spencer  
Online coordinator for UK NATIONAL LOTTERY

to



## Lottery – Social Engineering

---

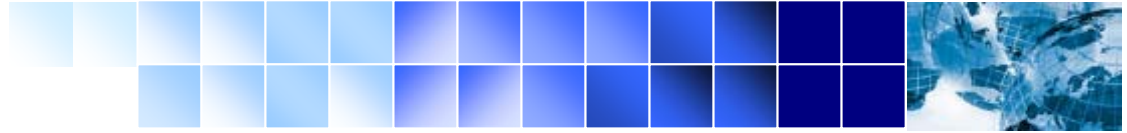
For security reasons, you are advised to keep your winning information confidential till your claims is processed and your money remitted to you in whatever manner you deem fit to claim your prize. You can go to our online result site to confirm the value of your winnings and also get a prize breakdown:-

**Beware of Phishing Attacks**

[www.national-lottery.co.uk/player/p/results/results.do](http://www.national-lottery.co.uk/player/p/results/results.do)

<http://www.lottery.merseyworld.com/>

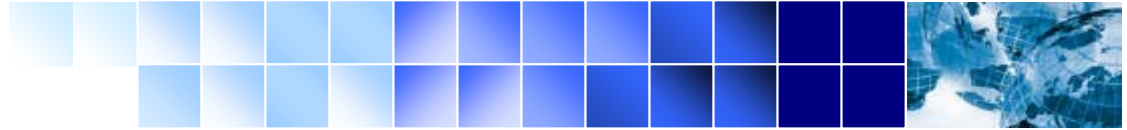
Goodluck from me and members of staff of the UK  
NATIONAL LOTTERY



# Phishing

- ▶ **Use of Email messages and Web pages that are replicas of existing sites to fool users into submitting:**
  - personal,
  - financial or
  - password data.





# Example of Phishing Email

Raw IP Address

Verify Your Information On Amazon

File Edit View Tools Message Help

Reply Reply All Forward Print Delete Previous

**From:** Amazon Billing Help  
**Date:** Wednesday, November 17, 2004 7:47 PM  
**To:**  
**Subject:** Verify Your Information On Amazon

**amazon.com.**

**Dear Amazon Member,**

Due to recent account takeovers and unauthorized listings, Amazon is introducing a new account verification process. From time to time, randomly selected accounts (seller and/or buyer) are subjected to an advanced verification process based on our merchant accounts/bank relations and customer's credit card. Amazon may also request in an email message scanned/faxed copies of one or more photo ID's. Your account confirmation may fail if your credit card/bank account is expired, or if you have changed your credit card number, billing address etc. without notifying us about the change. Subject of this verification process are also the accounts that have unpaid dues to Amazon.

Your account has not been suspended, but if within 48 hours after you receive this message your account is not confirmed we reserve the right to suspend your Amazon registration. If you received this notice and you are not the authorized account holder, please be aware that it is in violation of Amazon policy to represent oneself as another Amazon user. Such action may also be in violation of local, national, and/or international law. Amazon is committed to assisting 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 full extent of the law.

Note: If this is the second time you received this notice, it might be because you have made a mistake when you updated your details or that the account was not updated at all.

**To confirm your identity with us click here:**  
<http://signin.amazon.com/aw-cgi/amazonISAPI.dll?userconfirm&ssPageName=h:h:sin:US>

**We apologize in advance for any inconvenience this may cause you and we would like to thank you for your cooperation as we review this matter.**

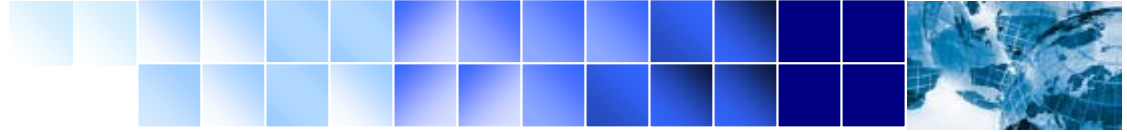
Respectfully,  
Trust and Safety Department  
Amazon Inc.

[Conditions of Use](#) | [Privacy Notice](#) © 1996-2004, Amazon.com, Inc. or its affiliates

<http://148.208.234.7/amazon/exec/obidos/flex-up-date/secure/.Mails/update.htm>

**This Email is Phish**

**How can you tell?** The easiest way to tell is by looking at the URL displayed on the status bar: 148.208.234.7 – the use of a raw IP address in a URL is always suspicious. More important is the recognition that Amazon, like many other e-commerce vendors, doesn't put links in their emails for login purposes. If Amazon did have a problem with your account they would have instructed you to go to their web site and login there.



## Example of Phishing Email

---

**MCB Internet Banking <online.alert@mcb.mu>**

01/30/2007 10:00 PM To: xyz@domain.com

CC:

Subject: Warning Message From Mauritius Commercial Bank Ltd

Account Trouble

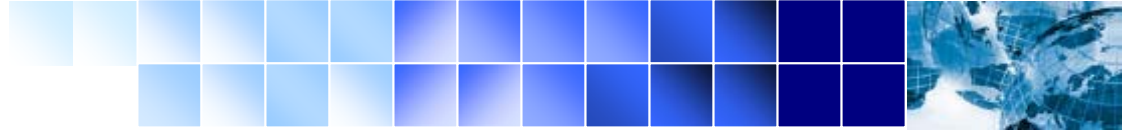
We are contacting you to remind you that on 20.01.2007 our Account Review Team identified some unusual activity in your account. In accordance with The Mauritius Commercial Bank Ltd User Agreement and to ensure that your account has not been compromised, access to your account was limited. Your account access will remain limited until this issue has been resolved please log in your account or click on the link below:

[my account activity](#)

---

Please do not reply to this automatically generated email message.

**Beware of Phishing Attacks**



# Phishing

---

## Prevention

- ▶ **Don't give out personal information**
- ▶ **Ensure you are on the right website with the right web address**
- ▶ **Use anti-phishing software – IE7 and Mozilla Firefox 2.0 includes a form of anti-phishing technology**



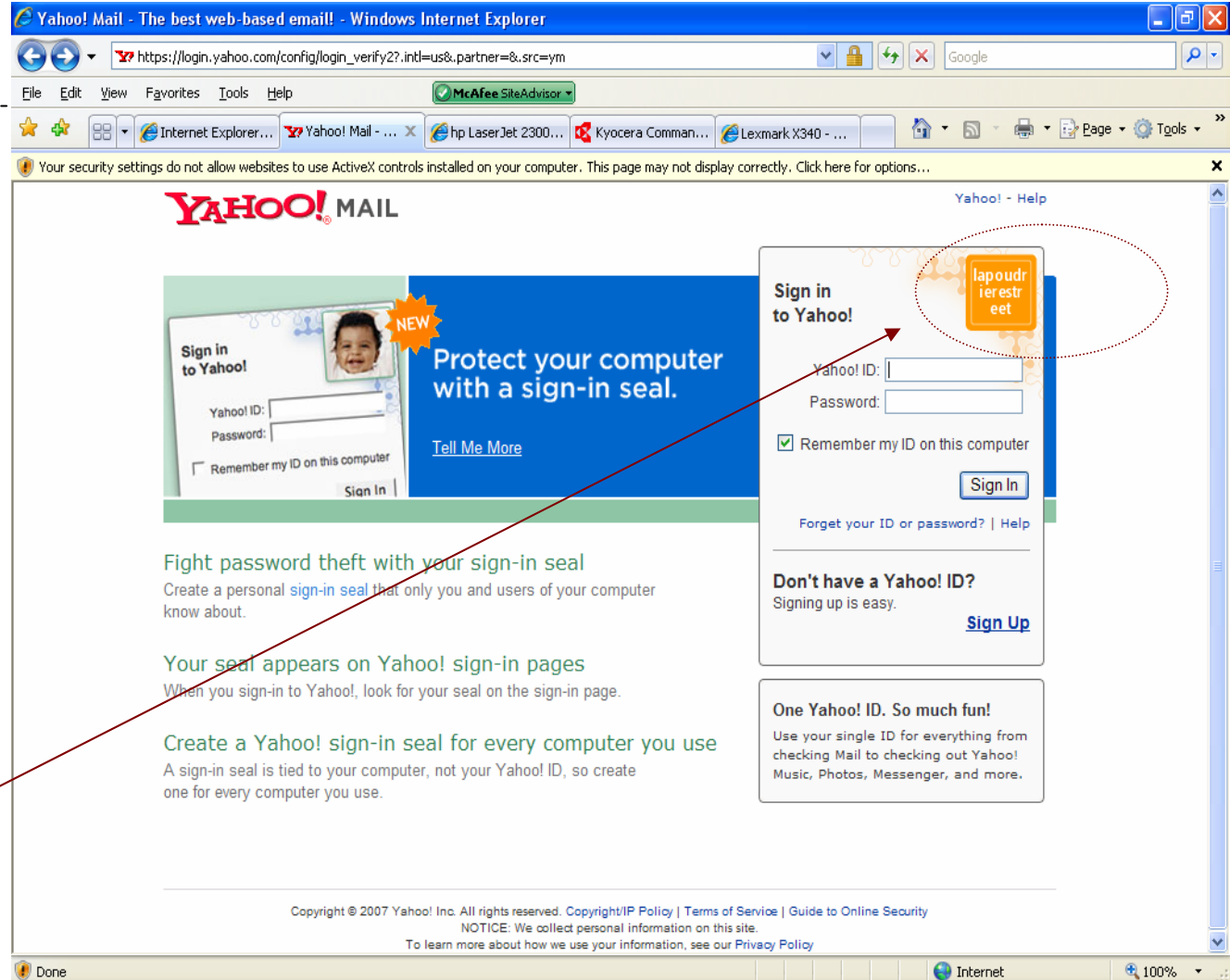


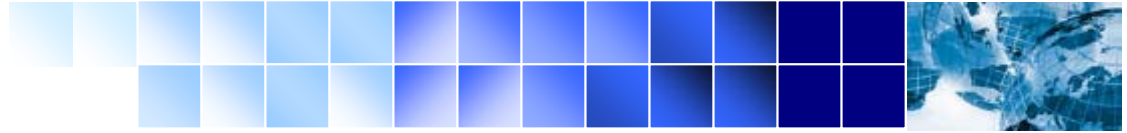
# Phishing

## Prevention

Some website already offers password theft prevention mechanism

Sign-in seal





# Sophistication of Attacks

---



## U.S. Department of Justice Federal Bureau of Investigation

---

For Immediate Release  
February 22 , 2005

Washington D.C.  
FBI National Press Office

### FBI ALERTS PUBLIC TO RECENT E-MAIL SCHEME

*E-mails purporting to come from FBI are phony*

Washington, D.C. - The FBI today warned the public to avoid falling victim to an on-going mass e-mail scheme wherein computer users receive unsolicited e-mails purportedly sent by the FBI. These scam e-mails tell the recipients that their Internet use has been monitored by the FBI's Internet Fraud Complaint Center and that they have accessed illegal web sites. The e-mails then direct recipients to open an attachment and answer questions. The attachments contain a computer virus.

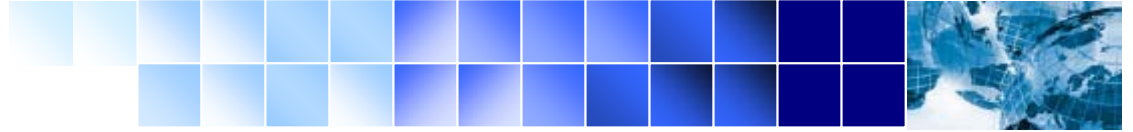
These e-mails did not come from the FBI. Recipients of this or similar solicitations should know that the FBI does not engage in the practice of sending unsolicited e-mails to the public in this manner.



## Conclusion

---

- ▶ **Avoid giving unnecessary information online (e.g. subscribing to a newsletter whereby your personal details are requested)**
- ▶ **Be sure you are dealing with someone or a site that you know and trust before giving out personal information**
- ▶ **Use regularly updated antivirus and antispyware software**
- ▶ **Use client filters or ISPs based filters**



---

**Thank You**