


International Telecommunication Union

## Threats to the Information Society

### Phishing & Identity Theft

Alexander NTOKO  
Chief, E-Strategies Unit  
International Telecommunication Union (ITU)  
Geneva, Switzerland

ITU Telecommunication Development Bureau (BDT) – E-Strategies Unit. Page - 1



International Telecommunication Union

## Why are we doing it? – Mandate

- Decisions of ITU Member States adopted at the World Telecommunication Development Conferences (WTDC 2002 and 2006) – Istanbul and Doha Action Plans (IsAP) Programme 3.
- Outcome of the World Summit on the Information Society (WSIS) – Summit for Heads of States resulting in the Geneva Plan of Action and Tunis Agenda – ITU as sole moderator/facilitator in the implementation WSIS Action Line C.5 – Cybersecurity including cybercrime.
- Enhance security and build confidence in the use of public networks for e-services/applications...
- Provide assistance to Member States in developing laws and model legislation for e-services/applications, prevention of cyber crime, security, ethical issues and data privacy ...
- Identify security requirements and propose solutions for the development of secure IP infrastructure for e-services/applications on various types of networks using relevant technologies ...
- Develop tools to facilitate the exchange of best practices on IT security, legal issues related to the areas of activity of this Programme.
- It is necessary to address the security concerns in order to leverage the potentials of public networks as vehicles for delivering affordable value-added e-services/applications ...
- Act as a facilitator for regional and interregional cooperation, and support appropriate capacity-building activities at the regional level.

ITU Telecommunication Development Bureau (BDT) – E-Strategies Unit. Page - 2



International Telecommunication Union

## Cybercrime threats on the rise, says Symantec

### LATEST ATTACKS ARE DESIGNED TO STEAL DATA

By Mike Al-Sinani  
10/17/2009

**Key Findings**

- Bot-infected computers increasing in China
- Phishing threats, which deceive users into revealing confidential information, continued to rise during the second half of 2009, despite 750 million daily phishing attempts were identified, an increase of 5.20 per cent over the first half.
- Symantec documented 895 new software vulnerabilities, the largest number of vulnerabilities ever filed.
- Symantec expects that the commercialization of vulnerability research will increase.
- Code developers may opt to modify currently circulating source code rather than developing new threats.

... but is cybercrime an issue for developing countries?

ITU Telecommunication Development Bureau (BDT) – E-Strategies Unit. Page - 3



International Telecommunication Union

## ... but is cybercrime an issue for developing countries?

ITU Telecommunication Development Bureau (BDT) – E-Strategies Unit. Page - 4




International Telecommunication Union

developing countries are embarking on e-government, e-business and e-payment solutions. With no geographical borders in the information society, ... *How vulnerable are (or will be) online users to phishing and identity theft?*

- Receiving online submissions to renew national identity cards:  
*Am I dealing with the owner of the identity card?  
How do I know this is really a government site?*
- Submitting confidential bids for government procurements:  
*Is the bid from a registered company?*
- Transmitting sensitive government documents online.  
*Can an unauthorized person view the document?  
How can access control be ensured?*

ITU Telecommunication Development Bureau (BDT) – E-Strategies Unit. Page - 5



International Telecommunication Union

- Issuing birth certificates and land certificates via the Internet:  
*Can a citizen assume another person's identity?  
What if that citizen then changes the owner field in a land certificate?*
- Conducting online elections via the Internet – e-voting:  
*How do we guarantee that this vote is from the legitimate (registered) user?*

ITU Telecommunication Development Bureau (BDT) – E-Strategies Unit. Page - 6

Citizens, governments and businesses conducting online transactions run the risk of having their Identities stolen...

### What is Identity Theft?

- Identity theft occurs when somebody steals your name and other personal information for fraudulent purposes. Identity theft is a form of identity crime (where somebody uses a false identity to commit a crime).
- The act of impersonating another, by means of using the person's information, such as birth date, address, name, and other personal information.
- Identity theft is the deliberate assumption of another person's identity, usually to gain access to their finances, privileges, immigration purposes or frame them for a crime.

ITU Telecommunication Development Bureau (BDT) – E-Strategies Unit. Page - 7

### Phishing and Identity Theft

#### What is Phishing?

- Phishing (also called brand spoofing or carding) is a technique for acquiring your personal information and subsequently committing fraud in your name, including stealing your identity.
- Use of social engineering plus malware/crimeware (e.g., Trojans) to steal identity mostly for fraudulent purposes.
- It's a form of cyber-crime growing faster than the ability of the police or courts to deal with it.
- About **10 years old** but attacks are increasing and getting more sophisticated.
- "phishing" originated from the word "fishing". Like in real fishing, scammers lure victims using baits to divulge information that is used for fraudulent purposes.

ITU Telecommunication Development Bureau (BDT) – E-Strategies Unit. Page - 8

### Phishing and Identity Theft

#### How is phishing perpetrated (typical scenario)?

- User receives Authentic-looking email - In a typical phishing attempt, you will receive an authentic-looking email message that appears to come from a legitimate organisation (bank, business partners or even your own employer).
- Email contains Link to a Website – Email will usually contain a link to a fake Website.
- User requested to click on the link to enter some information, or download a software (e.g., security update).
- Malware or crimeware downloaded from Website and is installed on user's computer.
- Downloaded software steals personal information using a wide range of techniques (e.g., Trojan-based keyloggers).

Phishing can also be perpetrated via **telephone (fixed and mobile) Instant Messaging**, and it is also possible for you to be phished by postal mail or even in person.

ITU Telecommunication Development Bureau (BDT) – E-Strategies Unit. Page - 9

### Who perpetrates it?

- Phishers or scam artists who send out millions of emails, realizing that even if only a few recipients have them enough identifying information, they can profit from the resulting fraud.
- Internet Service Providers who host phishing websites.
- According to APWG report of July 2006, USA still tops the list of countries hosting most of the web sites for phishing based keyloggers and Trojans.
- Between March and July 2006, APWG reports show a slight decrease in hosted websites in the US, decrease in Spain and China but significant growths in Portugal, Russia and Brazil. **What happened???**
- It is very likely that without efforts to combat this problem, more developing countries would be hosts to phishing sites.

ITU Telecommunication Development Bureau (BDT) – E-Strategies Unit. Page - 10

### Who perpetrates it?

**Phishing-based Keylogger and Trojan Downloads by Hosting Countries (by IP address)**  
The chart below represents a breakdown of the websites which were classified during April as hosting malicious code in the form of either a phishing-based keylogger or a Trojan downloader which downloads a keylogger. The United States is still the top geographic location with 27.7%. The rest of the breakdown was as follows: **Russia 19.17%, Brazil 6.1%, China 5.98%, Korea 4.6%, Germany 3.74%, Canada 3.24%, Portugal 3.11%, Italy 2.86%, Spain 2.74%.**

**Top 10 Phishing Based Keylogger and Trojan Downloaders by Hosting Country**

**Top 10 Phishing Based Keylogger and Trojan Downloaders by Hosting Country**

AntiPhishing Working Group Report of March 2006

AntiPhishing Working Group Report of July 2006

ITU Telecommunication Development Bureau (BDT) – E-Strategies Unit. Page - 11

### Phishing and Identity Theft - Trends


Attack Percentages

- 6.87 - 34.26
- 1.67 - 6.78
- 0.56 - 1.58
- 0.00 - 0.46

Phishing Reports Received July '05 - July '06

June 2006 showed the highest number of unique phishing attacks recorded by APWG

ITU Telecommunication Development Bureau (BDT) – E-Strategies Unit. Page - 12




## Phishing and Identity Theft

**Who is (or will be) affected by phishing?**

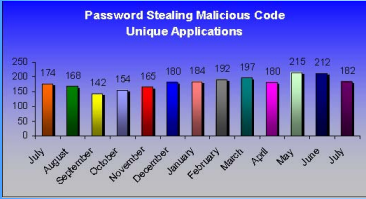
- Popular targets are users of online services. Any Internet users who's email or other personal records have been made available on any public forum or online service (e.g., e-government, e-business and e-banking).
- More online users in developing countries will be victims of phishing as countries embark on initiatives in e-government, e-business, e-banking and e-payments.
- Anyone who has personal information that can be used for online fraud is a potential victim of phishing.  
Example: More than 26 million US veteran records were stolen. Even if these veterans are not all online users, their identities can still be used for online fraud.

ITU Telecommunication Development Bureau (BDT) – E-Strategies Unit. Page - 13




## Phishing-based Trojans - Keyloggers

Crimeware code which is designed with the intent of collecting information on the end-user in order to steal those users' credentials. Unlike most generic keyloggers, phishing-based keyloggers have tracking components which attempt to monitor specific actions (and specific organizations, most importantly financial institutions and online retailers and ecommerce merchants) in order to target specific information, the most common are; access to financial based websites, ecommerce sites, and web-based mail sites.



Month	Number of unique Websites
July	174
August	168
September	142
October	154
November	165
December	180
January	184
February	192
March	197
April	180
May	215
June	212
July	182

ITU Telecommunication Development Bureau (BDT) – E-Strategies Unit. Page - 14




## Phishing-based Trojans

**DNS cache poisoning (Redirectors)**  
**Man-in-the-middle phishing (Pharming)**

**Redirectors:** Redirecting end-users network traffic to a location where it was not intended to go to by exploiting security vulnerabilities in the ISP DNS server to change hosts files and other DNS specific information. Pharming can be implemented through DNS cache poisoning.

**Pharming:** Intercepting information in between two parties' communications in order to redirect users to a fraudulent location. With the proliferation of unprotected and insecure wireless connections (e.g., WiFi) the effects of Pharming could be significant to the growing number of wireless users.

ITU Telecommunication Development Bureau (BDT) – E-Strategies Unit. Page - 15



## Phishing and Identity Theft — Example 1

\*\*\*  
05-Mar-2006


Scammers are taking advantage of the current US tax season.

\*\*\*

U.S government officials are warning of a growing online presence of phishing scams taking advantage of the current US tax season.

- Instead of banks or other financial institutions as the purported sender of these scams, the US IRS is being portrayed as the sender of the emails. It is believed the scams are regularly asking recipients for social security details and credit card details.
- IRS representatives say that their officials would never ask for such information via email.
- MillerSmiles News
- 05/03/06
- Talk about this article on our [phishing news discussion forum](#)

ITU Telecommunication Development Bureau (BDT) – E-Strategies Unit. Page - 16



## Phishing and Identity Theft — Example 2

From: abuse@itu.ch [mailto:abuse@itu.ch]  
Sent: Wednesday, June 14, 2006 9:08 PM  
To: Prasad, Pradeep  
Subject: Account Alert

Dear Valued Member,  
According to our terms of services, you will have to confirm your e-mail by the following link, or your account will be suspended within 24 hours for security reasons.  
<http://www.itu.ch/confirm.php?account=pradeep.prasad@itu.ch>  
<[http://211.97.61.61/Confirmation\\_Sheet.pdf](http://211.97.61.61/Confirmation_Sheet.pdf)>  
After following the instructions in the sheet, your account will not be interrupted and will continue as normal.  
Thanks for your attention to this request. We apologize for any inconvenience.

Sincerely,  
ITU Abuse Department

ITU Telecommunication Development Bureau (BDT) – E-Strategies Unit. Page - 17



## Phishing and Identity Theft — Example 3

You forwarded this message on 22.09.2005 20:10:

From: PostFinance [support@yellownet.ch]  
To: Nicko, Alexander  
Cc:  
Subject: Important Account Information Last Notice (ID: 028-1812995)

Dear PostFinance Valued Account Holder,  
PostFinance has a strict policy to ensure all of our customer's emails associated with their bank account(s) are confirmed. Upon inspection this email was registered with your account(s) however not confirmed. Please confirm your email by clicking the link below or if the link does not allow you to click on it please proceed by copying/pasting it into the appropriate web browsing window:

[https://www.yellownet.ch/start\\_e.html](https://www.yellownet.ch/start_e.html)

Email verification must be performed within 1 business day from receiving this email. Failure to comply will result in online banking suspension and limited account activity until an account specialist can contact you regarding this error. This can be avoided simply by following our online verification link above.

Sincerely,  
PostFinance, N.A. Account Services Department  
PostFinance, N.A. Member FDIC, Equal Housing Lender  
Copyright © 2005 PostFinance, N.A. All rights reserved.

[https://www.yellow-net.cc/start\\_e.html](https://www.yellow-net.cc/start_e.html)

ITU Telecommunication Development Bureau (BDT) – E-Strategies Unit. Page - 18




**Phishing and Identity Theft — Example 4**

In July, Websense® Security Labs discovered a new malicious website, which distributed malicious code that installs a Trojan Horse on end-users' machines. This potentially occurs without user interaction. The site appeared to be mimicking a World Cup 2006 Soccer website with the exception that they have a lead story regarding the now infamous, Zinedine Zidane head butt incident from the World Cup final against Italy. Upon visiting any of the pages on the site, end-users were potentially infected with a Trojan Horse downloader. This Trojan Horse downloads additional payload code from the site. The site was using the underground "Web Attacker" toolkit (discussed in an earlier alert <http://www.websense.com/resources/whitepapers/Attacker.html>). The Web Attacker toolkit is sold on a Russian website and costs anywhere from \$50 to \$500. This toolkit allows users to install code that exploits users based on their browser types. The installed code includes one of five different variants, including exploits for old and new vulnerabilities. This site was hosted in the United States.

Site screenshot:



ITU Telecommunication Development Bureau (BDT) – E-Strategies Unit. Page - 19



**General TRENDS**  
As it expands to other platforms, it's more difficult to detect

**Expansion to Mobile** - New type of phishing could hit mobile phone users. **Mophishing** is where hackers send out fake banking applications to unsuspecting mobile phone users. The users then type their account details into the application thinking they were accessing their accounts when they were actually sending their personal details back to the hacker.


ITU Telecommunication Development Bureau (BDT) – E-Strategies Unit. Page - 20



**Summary – July 2006**


- No. of unique phishing reports: **23670**
- Number of unique phishing sites: **14191**
- Country hosting the most phishing websites in July: **United States**
- Contain some form of target name in URL: **46%**
- Average time online for site: **4.8 days**

ITU Telecommunication Development Bureau (BDT) – E-Strategies Unit. Page - 21



Could Affect various Sectors  
Knows No Geographical or Time barriers  
More and more Sophisticated  
More than 90% linked to Websites  
Average duration of website **5 days**

ITU Telecommunication Development Bureau (BDT) – E-Strategies Unit. Page - 22



**CONCLUSION**

Even though Internet penetration and usage are still relatively low in some countries in this sub-region, now is the time to start taking seriously the challenges brought about by cybercrime as countries increase their reliance on ICTs for social and economic development and as they embark on efforts to build ICT platforms some of which will be delivering critical services to businesses and citizens.

In addition to legislation and enforcement mechanisms, **identity management and verification** is a vital technology solution in the fight against phishing and identity theft.

ITU Telecommunication Development Bureau (BDT) – E-Strategies Unit. Page - 23



**Thank You for Your Attention**  
**For further information:**

<http://www.itu.int/ITU-D/e-strategies>  
[e-strategies@itu.int](mailto:e-strategies@itu.int)

ITU Telecommunication Development Bureau (BDT) – E-Strategies Unit. Page - 24