

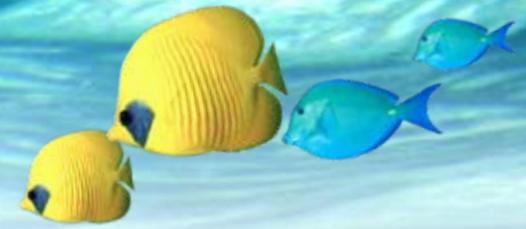


# *Department of Energy Cyber Security Program*

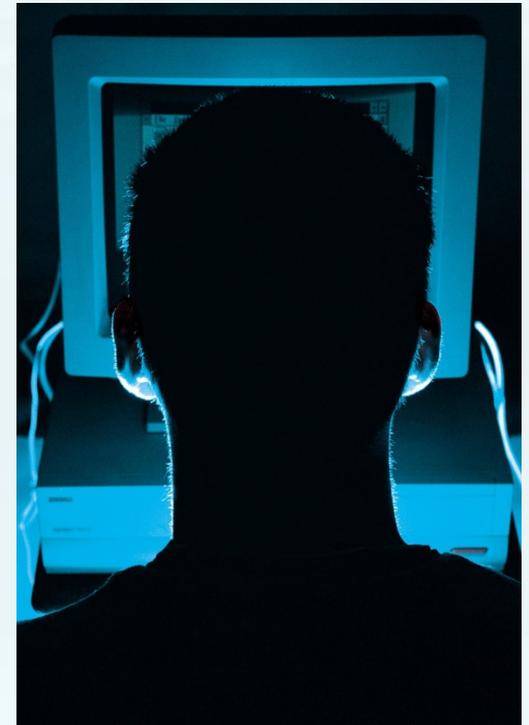
## **Anti-Phishing Awareness Brown Bag Presentation**

**Tuesday, May 20, 2008**

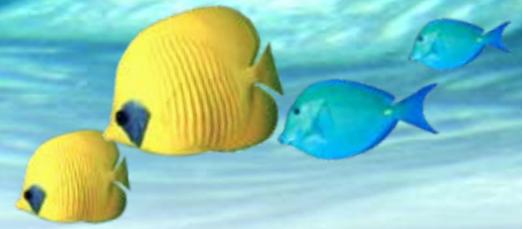
# What is Phishing?



- Cyber criminals send fraudulent emails to unsuspecting users luring them into revealing sensitive information
- There are many forms of phishing, but they all have the same purpose:
  - To trick users into divulging sensitive information



# Presentation Goal

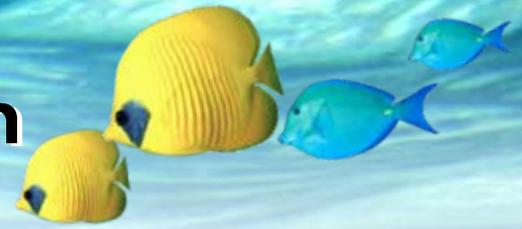


- To give you information you can use today both at home and at work to recognize and avoid phishing attacks
- The most effective tool in fighting phishing is user awareness

Awareness is the Key  
To Prevention



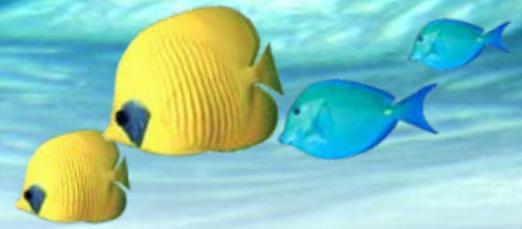
# OCIO Anti-Phishing Campaign



- Anti-Phishing Awareness Campaign currently underway
- Posters, newsletters, novelty items, events, OCIO Web page
- Goal: Fight phishing through increased user awareness



# Today's Menu



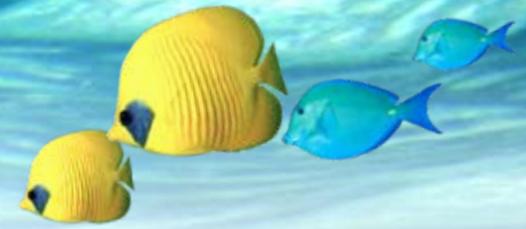
- How phishing attacks work
- Examples of phishing attacks
- Filleting a phish
- 6 tips for fighting phishing
- What to do if you are attacked
- Where to go for more information



Never trust anything in  
an unsolicited email from  
someone you don't know...

No matter how legitimate  
the email looks.

# Phishing: Urgency



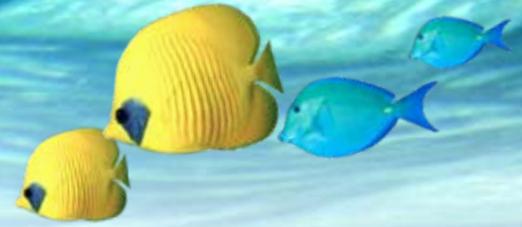
## **WARNING!**

Someone has attempted to log onto  
your Citibank account.

You must log on to verify your account information  
**immediately**  
or your account will be closed.

Phishing attacks employ a **sense of urgency** to scare recipients into responding quickly, before they have time to stop and think.

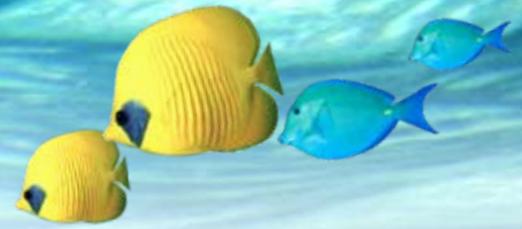
# How Does Phishing Work?



- There are two methods used in most phishing email attacks:
  1. You click on a link to enter your personal information
  2. Simply opening an email or attachment installs spyware on your computer

The spyware works behind the scenes to steal sensitive information

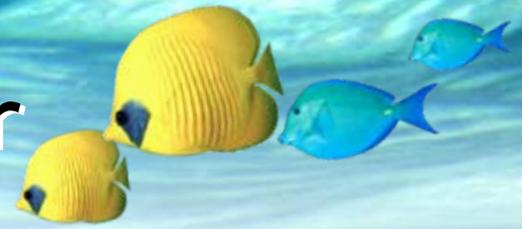
# What is at Risk?



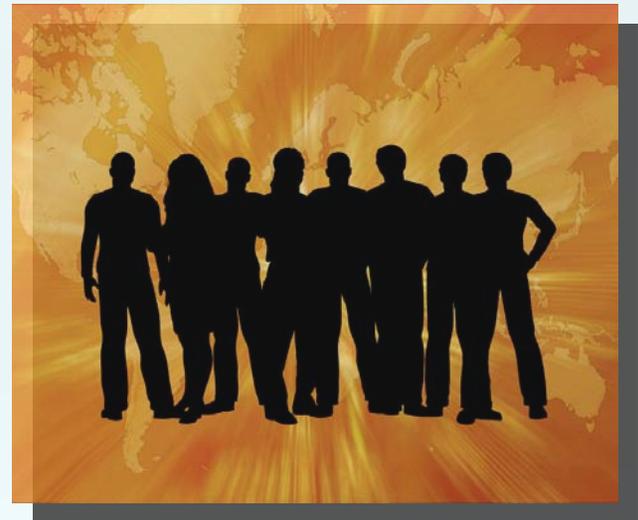
- DOE sensitive information
  - Your identity
  - Your credit history
  - Your bank account and credit cards
- 
- 3.6 million people in the U.S. lost \$3.2 billion to phishing scams in 2007



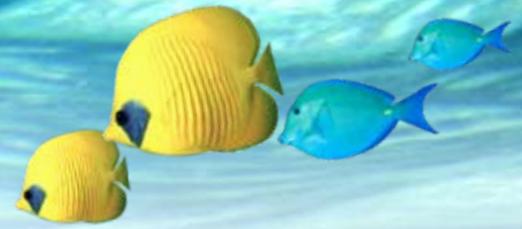
# Profile: Phishing Attacker



- The enemies of the United States are highly skilled in cyber warfare
- Phishing attackers include:
  - Script kiddies
  - Cyber criminals
  - State-sponsored cyber terrorists
- U.S. government agencies are prime targets for phishing attacks



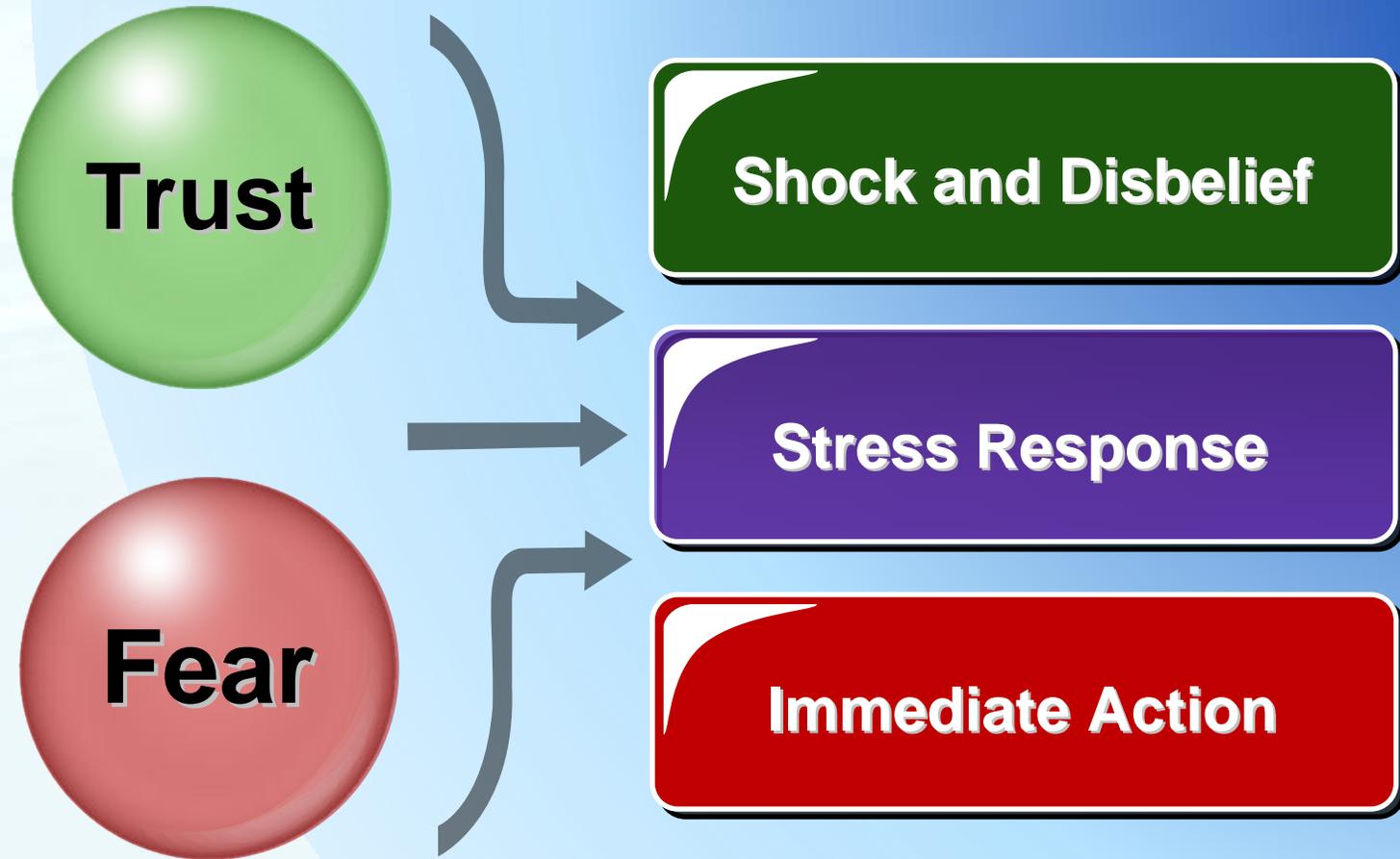
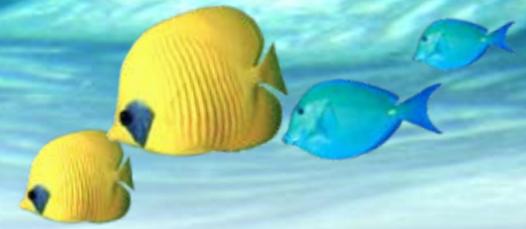
# Profile: Phishing Victim



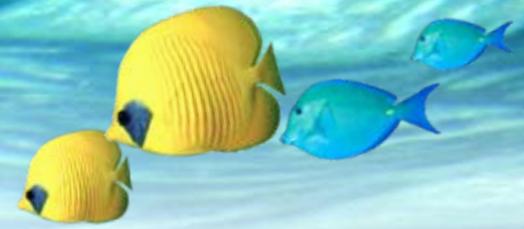
- You are a potential target for a phishing attacks if you:
  - Use a computer at work or home
  - Send and receive email
- Most phishing attacks are broadly dispersed
- Bottom Line:  
No one is immune from phishing attacks



# Psychological Triggers



# Forms of Phishing



- **Spear Phishing**

- Targeted phishing attacks
- Includes information tailored to the victim

- **Vishing (Voice Phishing)**

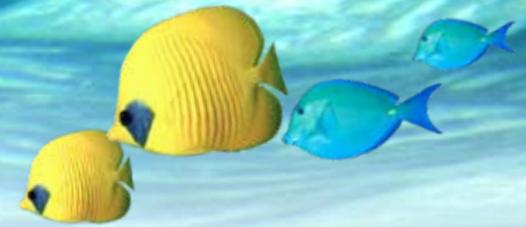
- User is prompted by phish email to call bogus number and disclose sensitive information

- **Whaling**

- Spear phishing targeted specifically to executives



# Recent Whaling Attack



- In April 2008, thousands of business executives received fake subpoenas via email to appear in U.S. District Court
- More than 1,800 clicked on the message
- Link ends in .com, not .gov
- Key logger Trojan software installed

AO 88(Rev.11/94) Subpoena in a Civil Case



Issued by the  
**UNITED STATES DISTRICT COURT**

Issued to: [REDACTED]

**SUBPOENA IN A CIVIL CASE**

Case number: 45-616-RRE  
United States District Court

**YOU ARE HEREBY COMMANDED to appear and testify before the Grand Jury of the United States District Court at the place, date, and time specified below.**

**Place:** United States Courthouse  
880 Front Street  
San Diego, California 92101

**Date and Time:** May 9, 2008  
9:00 a.m. PST

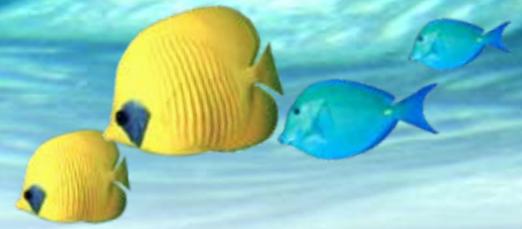
**Room:** Grand Jury Room  
room 5217

**Issuing officers name and address:** O'Mevely & Meyers LLP; 400 South Hope Street, Los Angeles, CA 90071

[Please download the entire document on this matter \(follow this link\) and print it for your record.](#)

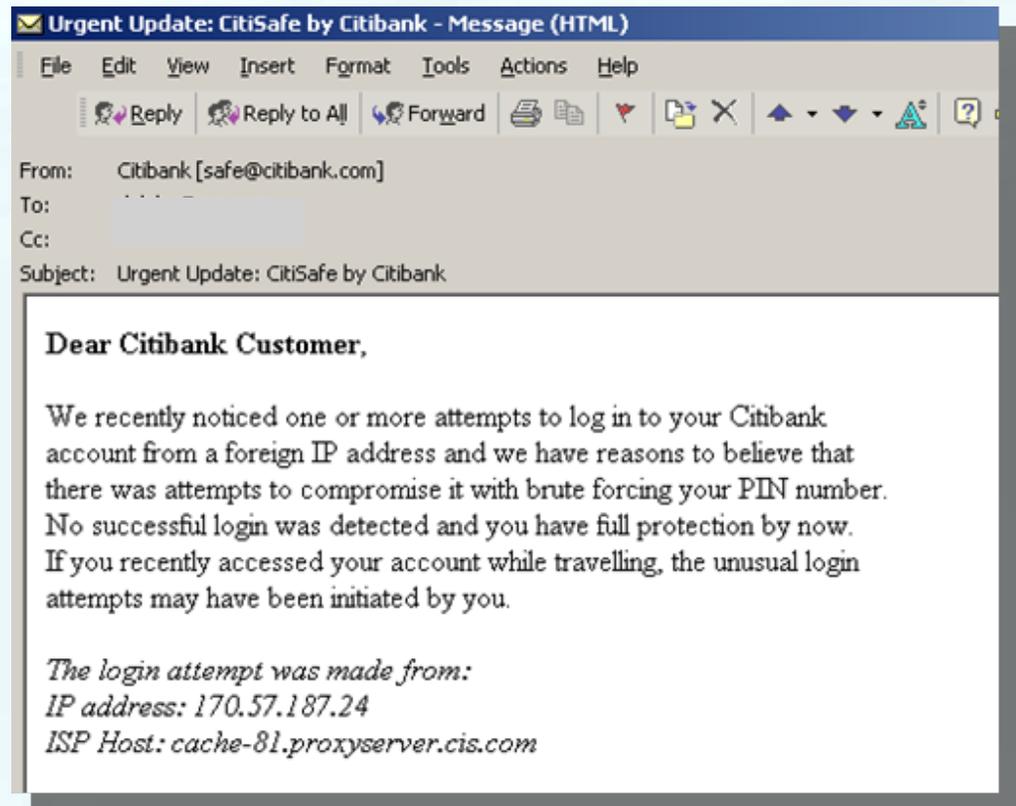
This subpoena shall remain in effect until you are granted leave to depart by the court or by an officer on behalf of the court.

# 1st Generation Phish

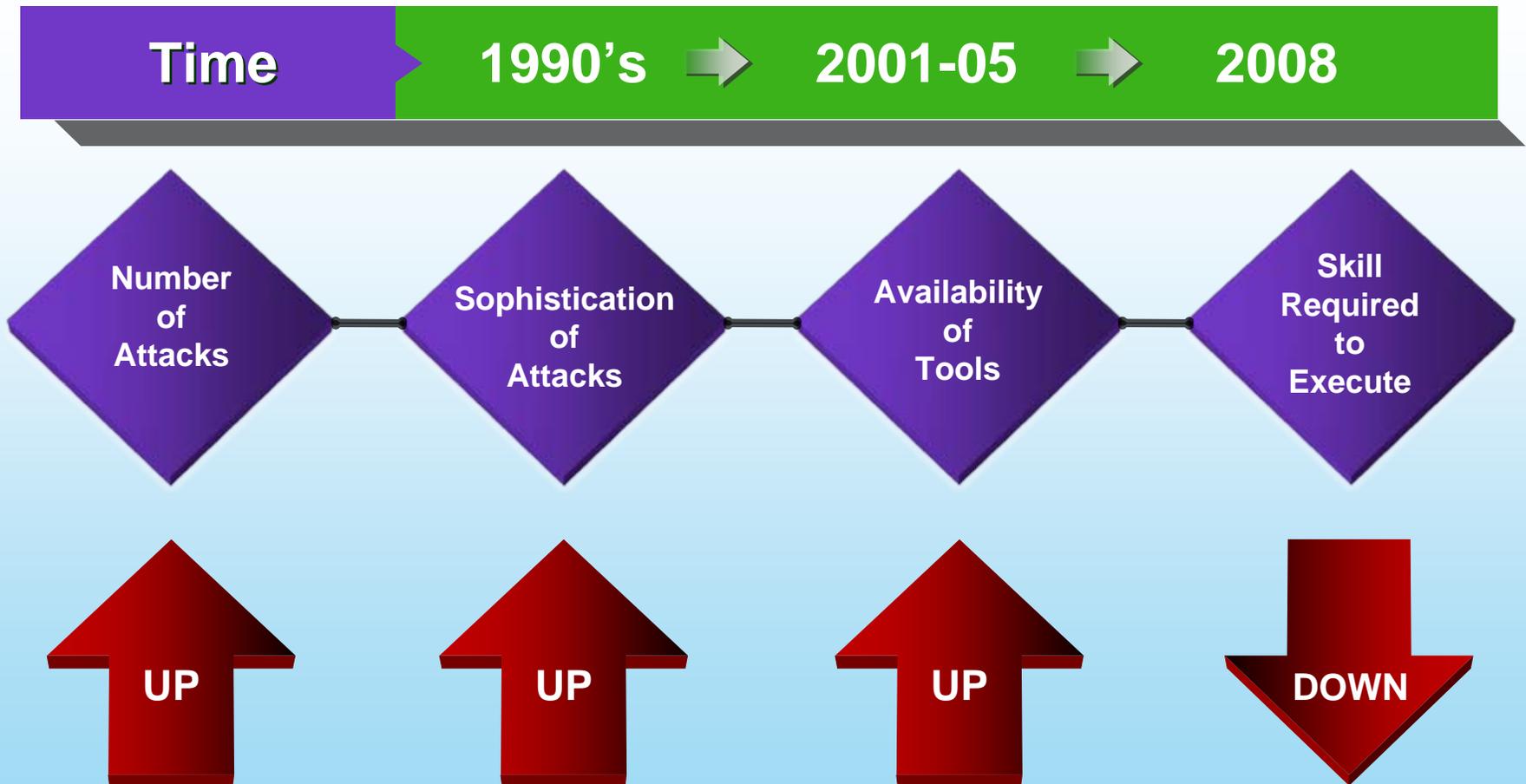
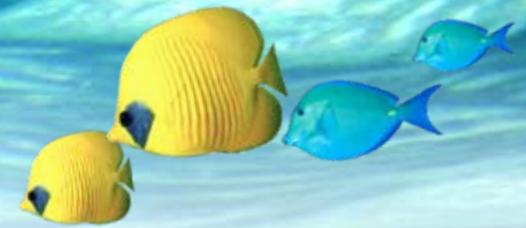


- **Target: Citibank**

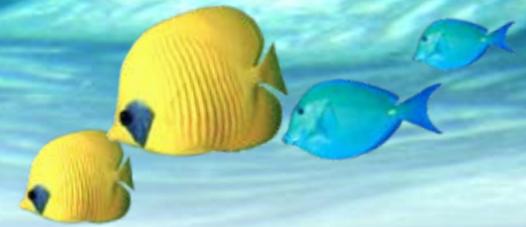
- No graphics, just a link to a Website
- Typos, errors in grammar
- Always present: **A sense or urgency**



# Evolution of Phishing



# Next Generation Phish



Real logo



**Your account will be suspended !**

Few typos

Dear SunTrust Customer,

In accordance with our major database relocation, we are currently having major adjustments and updates of user accounts to verify that the informations you have provided with us during the sign-up process are true and correct. However, we have noticed some discrepancies regarding your account at SunTrust. Possible causes are inaccurate contact information and invalid logout process.

Link to fraudulent website

We require you to complete an account verification procedure as part of our security measure.

You must click the link below to securely login and complete the process.

[Click here to reactivate your account](#)

Account suspension threat

Choosing to ignore this message will result in a temporary suspension of your account within 24 hours, until you will choose to solve this unpleasant situation.

Thank you for using SunTrust!  
The SunTrust Team

Valid website links

Please do not reply to this e-mail. Mail sent to this address cannot be answered. For assistance, [log in](#) to your SunTrust account and choose the "Help" link in the footer of any page.

## Protect Your Account Info

- **Make sure you never provide your password to fraudulent websites:** To safely and securely access the SunTrust website or your account, be sure to verify the link found in the address bar. This must be <https://www.suntrust.com>.

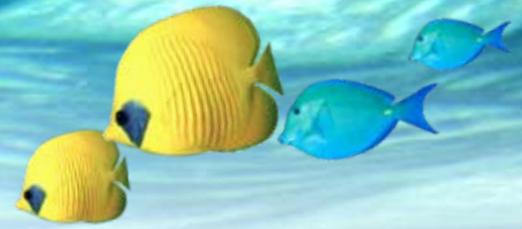
- **Don't share personal information via email:** We will never ask you to enter your password or financial information in an email or send such information in an email. You should only share information about your account once you have logged in to <https://www.suntrust.com/>.

## Protect Your Password

- **Never share your SunTrust password:** SunTrust representatives will never ask you for your password. If you believe someone has learned your password, please change it immediately and [contact us](#).

- **Keep your SunTrust password unique:** Don't use the same password for **SunTrust** and other online services such as AOL, eBay, MSN, or Yahoo. Using the

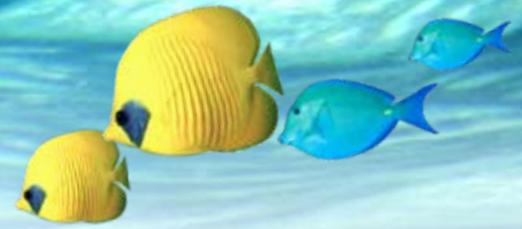
# School of Phish Pop Quiz



**Phishing is:**

- a. Another name for the activity of catching fish**
- b. A great way to spend the weekend**
- c. A form of computer fraud designed to trick people into disclosing sensitive information**

# School of Phish Pop Quiz



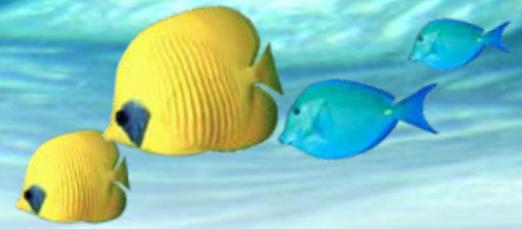
**Phishing attacks work by the following method:**

**a. Several schools of feisty fish batter unsuspecting swimmers**

**b. Cyber criminals use coercion and perceived authority to obtain sensitive information through fraudulent emails**

**c. Not sure**

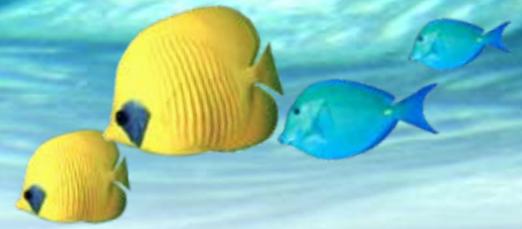
# School of Phish Pop Quiz



**Phishing scams trick users into divulging:**

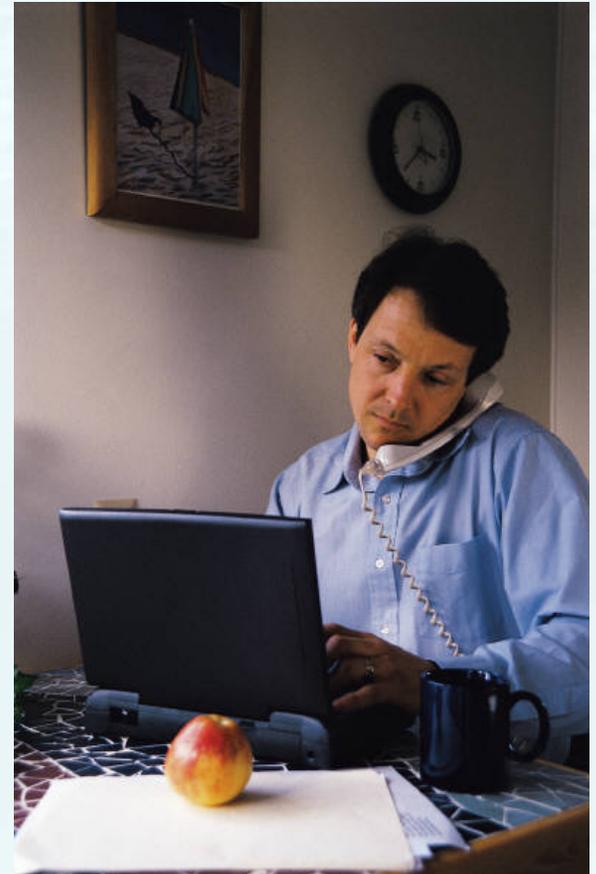
- a. Credit card information**
- b. Social security numbers**
- c. Bank account and PIN numbers**
- d. Other sensitive information**

# Filleting a Phish: eBay

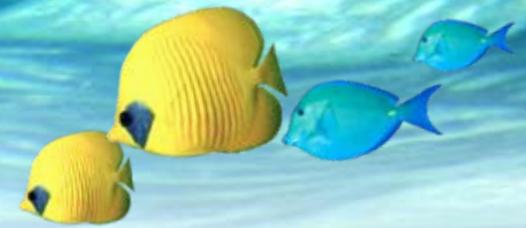


- Filleting a Phish: 
- I received an urgent email claiming to be from eBay
- “You eBay account has been locked”
- We will look at the code behind the attack to see how it works

**Warning!**  
Do Not Try This Yourself!



# Filleting a Phish: eBay



## Exhibit 1: eBay Phish Email



[? 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

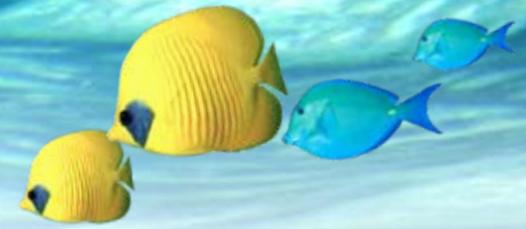
[http://signin.ebay.com/aw-c\\_gi/eBayISAPI.dll?Verify](http://signin.ebay.com/aw-c_gi/eBayISAPI.dll?Verify)

Regards,

eBay Member Service

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

# Filleting a Phish: eBay



- **Characteristics that help to build trust**
  - Use of actual eBay logo
  - Look and feel of actual eBay webpage
  - Use of eBay web links

The screenshot shows an email from eBay with the following content:

**ebay** 

[? 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

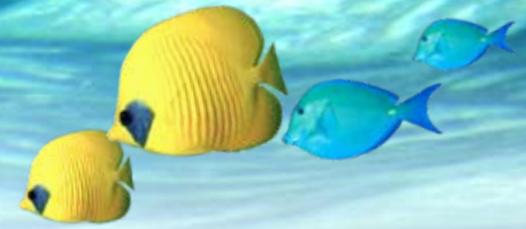
[http://signin.ebay.com/aw-c\\_gi/eBayISAPI.dll?Verify](http://signin.ebay.com/aw-c_gi/eBayISAPI.dll?Verify)

Regards,

eBay Member Service

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

# Filleting a Phish: eBay



## ❖ Links in phish emails are usually phony

- Links appears to be real, as is the link in our eBay phish
- Link appears to go to a site on eBay.com
- But when you click on this link, you go somewhere else
- How do they do this?



Dear eBay User,

We regret to inform you, that we had to block your eBay acc because we have been notified that your account may have b

Our terms and conditions you agreed to state that your acco or those you designate at all times. We have noticed some a indicates that other parties may have access and or control (

Please be aware that until we can verify your identity no furth allowed.As a result,Your access to bid or buy on eBay has b account fully,Please uptake and verify your information by cli

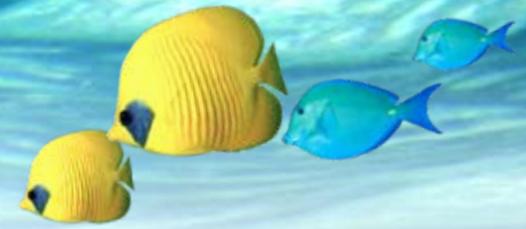
<http://signin.ebay.com/aw-c qi/eBay!SAPI.dll?Verify>

Regards,

eBay Member Service

\*\*Please Do Not Reply To This E-mail As You Will Not Rece

# Filleting a Phish: eBay



## ❖ HTML (HyperText Markup Language)

- HTML is the basic code behind all Web pages

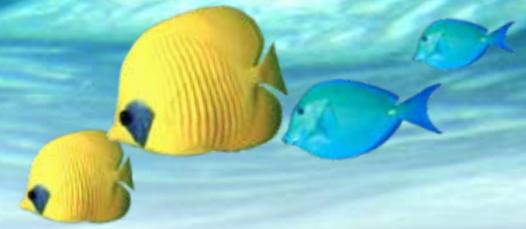
The Web link (or hyperlink) appears like this in our phish email...

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

But this is the actual HTML code that is behind that same link.

```
<a href="http://signin_ebay_com_account.barami.co.kr:7308/ebay.htm">  
http://signin.ebay.com/aw-cgi/eBayISAPI.dll?Verify</a></font></P>
```

# Filleting a Phish: eBay



❖ Let's take a closer look at that code:

URL (Link) for Internet site where you are sent



```
<a href="http://signin_ebay_com_account.barami.co.kr:7308/ebay.htm">  
http://signin.ebay.com/aw-cgi/eBayISAPI.dll?Verify  
</a></font></P>
```

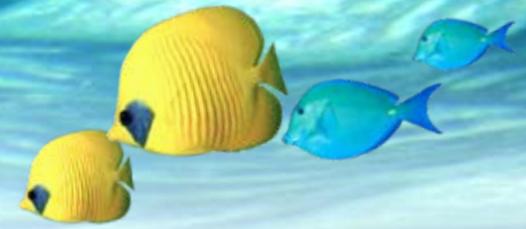


Hypertext string: What shows up  
in your browser

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



# Filleting a Phish: eBay

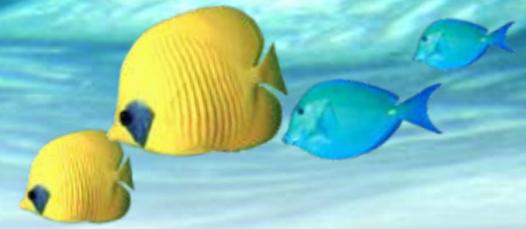


## ❖ Country Code Top Level Domains (ccTLDs)

- TLD is what comes after the . (gov, com, mil, org, edu, country codes)
- Web sites from other countries use ccTLDs
  - Example: [www.amazon.de](http://www.amazon.de) (Germany)

The screenshot shows the top navigation bar of the Amazon.de website. At the top left, there is a promotional banner for 'Neu: SPIELWAREN' with a 'Hier klicken' link and a small dog icon. The main navigation bar includes the 'amazon.de' logo, a shopping cart icon, and links for 'WUNSCHZETTEL', 'MEIN KONTO', 'HILFE', and 'IMPRESSUM'. Below this is a secondary navigation bar with category buttons: 'HOME', 'MEIN SHOP', 'BÜCHER', 'ENGLISH BOOKS', 'ELEKTRONIK & FOTO', 'MUSIK', 'DVD', 'VHS', 'SOFTWARE', 'PC- & VIDEO-SPIELE', 'KÜCHE, HAUS & GARTEN', and 'SPIELWAREN & KINDERWELT' (marked with a 'NEU' star). A third navigation bar contains red buttons for 'INTERNATIONAL', 'BESTELLEN LEICHT GEMACHT', 'TOPSELLER', 'PREIS-HITS', 'GUTSCHEINE', and 'JETZT VERKAUFEN'. The search bar features a 'SCHNELLSUCHE' label, a search input field, a dropdown menu set to 'Alle Produkte', and a 'LOS' button. At the bottom, a yellow banner states 'Kostenlose Lieferung ab 20 EUR. Bücher versandkostenfrei! Mehr dazu.'

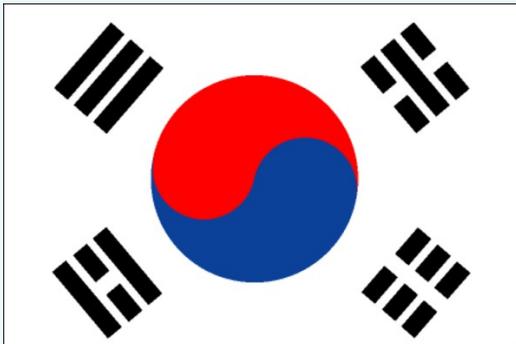
# Filleting a Phish: eBay



- ❖ HTML code behind link shows true location of Website you are linking to:

```
<a href="http://signin_ebay_com_account.barami.co.kr:7308/ebay.htm">
```

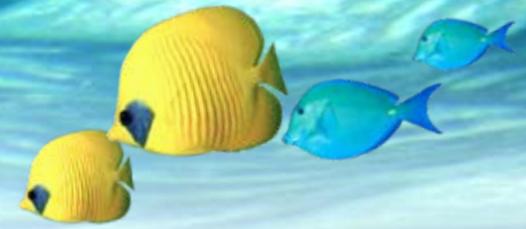
- eBay does not have Websites in Korea for its U.S. customers!



**Republic of Korea!**

For a full list of country codes, visit [www.iana.org](http://www.iana.org)

# Recent IRS Phishing Scam



- Users have reported receiving this phish email recently claiming to be from the IRS
- Links to a phony website which prompts you to enter your credit card information
- There are several variants, including a vishing attack

**Internal Revenue Service IRS.gov**  
DEPARTMENT OF THE TREASURY

Home | Get Tax Refund on your Visa or MasterCard | Refund Help

**Tax Refund**

**Get Tax Refund on your VISA or MasterCard**

Please enter your Social Security Number and a valid VISA or MasterCard number where you want the refund to be made.  
\*See our [Privacy Notice](#) regarding our request for your personal information.

**Social Security Number** ▶  
or IRS Individual Taxpayer Identification Number [shown on your tax return](#)

-  -

**Credit Debit Card** ▶

**Name on card:**

**Card Number:**

**Expiration Date:** Month  Year

**CVV Code:**  

**ATM Card PIN:**

**Refund Amount** ▶

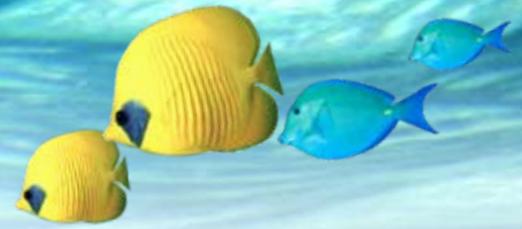
\$ 63.80

**Submit**

▶ Note: For security reasons, we recommend that you close your browser after you have finished the refund process.

[IRS Privacy and Security Policy](#)

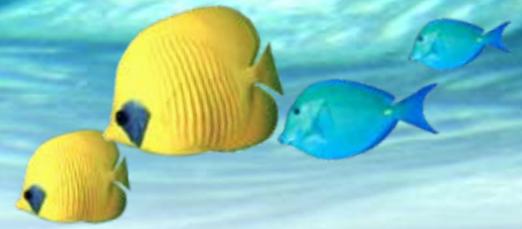
# 6 Tips to Fight Phishing



- 1. If you receive an email or pop-up message that asks for personal or financial information, do not reply.**
- 2. Don't email personal or financial information.**
- 3. Be cautious about opening attachments or downloading any files from emails.**



# 6 Tips to Fight Phishing

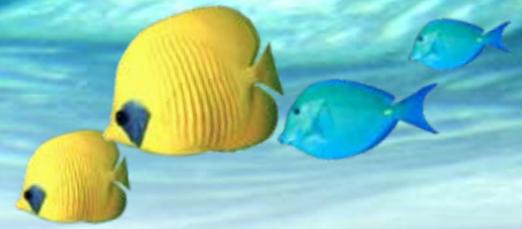


**4. Never enter your personal information in a pop-up screen.**

**5. Only open email attachments if you're expecting them and know what they contain.**



# 6 Tips to Fight Phishing

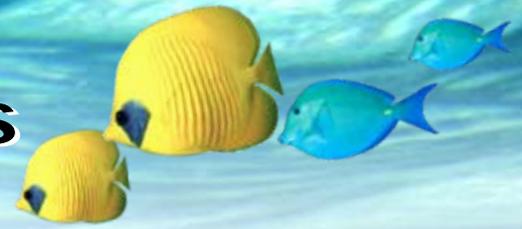


- 6. If you receive a suspicious email at work, don't open it, any attachments, or click on any links –**

**Contact the Helpdesk, 3-2500**



# Phishing Prevention Resources

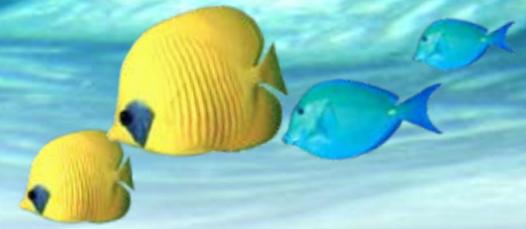


- [www.CIO.Energy.gov](http://www.CIO.Energy.gov)
- [www.FTC.gov](http://www.FTC.gov)
- [www.APWG.org](http://www.APWG.org)
- [www.fbi.gov/cyberinvest/escams.htm](http://www.fbi.gov/cyberinvest/escams.htm)

Awareness is the Key  
To Prevention



# Office of Cyber Security



- If you have questions about phishing prevention and awareness, or anything else related to the OCIO's cyber security program, please send us an email:

[Cyber.Security@hq.doe.gov](mailto:Cyber.Security@hq.doe.gov)

If you think twice  
Before you click,  
Then you won't fall  
For phishing tricks.

Avoid getting hooked

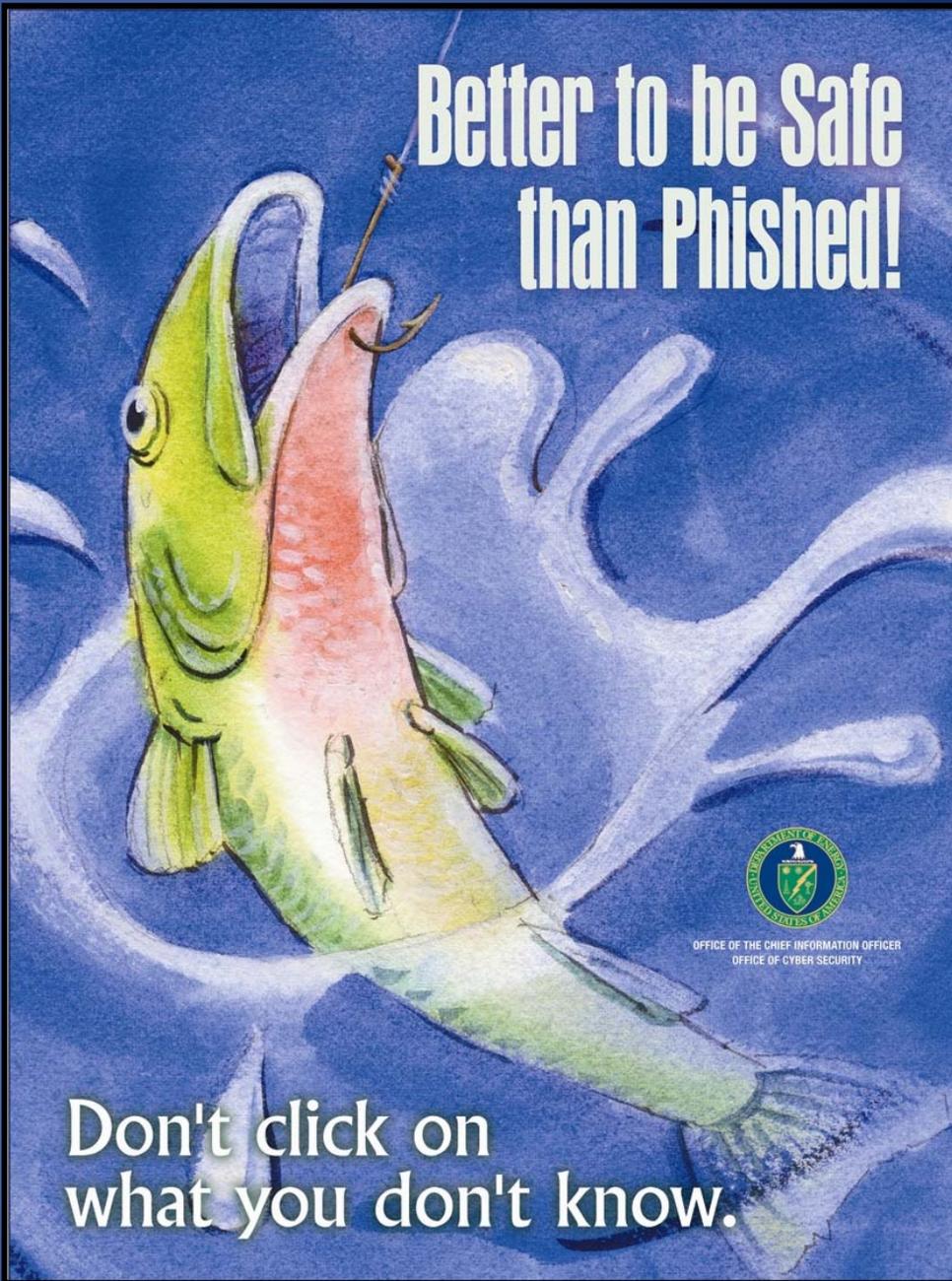
Before it's too late...

Fight phishing and

Don't take the bait.

# Thank You

Better to be Safe  
than Phished!



OFFICE OF THE CHIEF INFORMATION OFFICER  
OFFICE OF CYBER SECURITY

Don't click on  
what you don't know.