

# ***Headquarters Air Mobility Command***

---



## **Anti-Phishing Campaign Cyber Security Awareness Month**

**HQ AMC/A60H**

Located at: <https://eim.amc.af.mil/org/a6/default.aspx>

As of: 1 Oct 13

---

*We Answer the Call of Others...So They May Prevail*



# Objectives



- **Definition**
- **Threats**
- **Targets**
- **How they are doing it**
- **Phishing Indicators**
- **Protect Yourself**
- **Procedures on suspected phishing**





# Definition Of Phishing



phish·ing

'fiSHiNG/

noun: **phishing**

: a scam by which an e-mail user is duped into revealing personal or confidential information which the scammer can use illicitly



<http://www.merriam-webster.com/dictionary/phishing>

*We Answer the Call of Others...So They May Prevail*



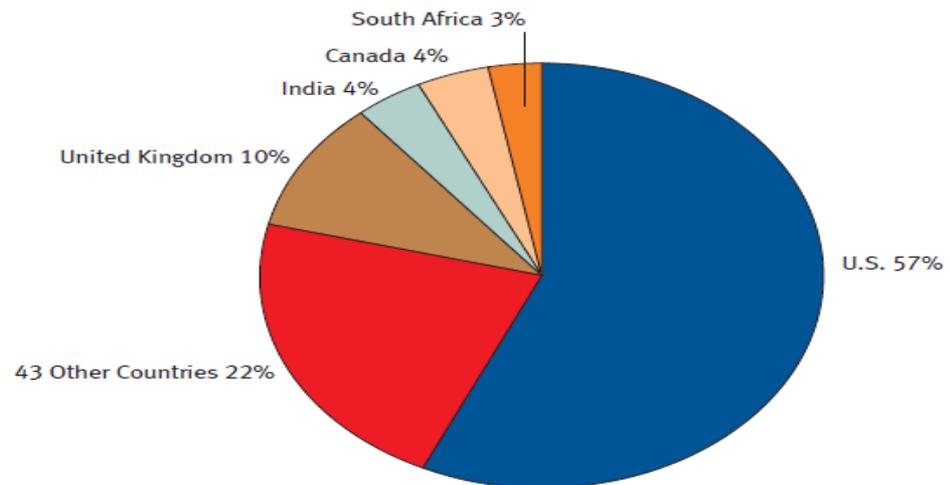
# Threats



- Phishing is still the top online threat
- In 2012, an average of 37,000 phishing attacks occurred each month
- losses from Phishing in 2012 = \$1.5 Billion+

## Top Countries by Attack Volume

The U.S. was targeted by phishing most in January – with 57% of total phishing volume. The UK endured 10%, followed by India and Canada with 4% of attack volume respectively.



Source: <http://www.emc.com>

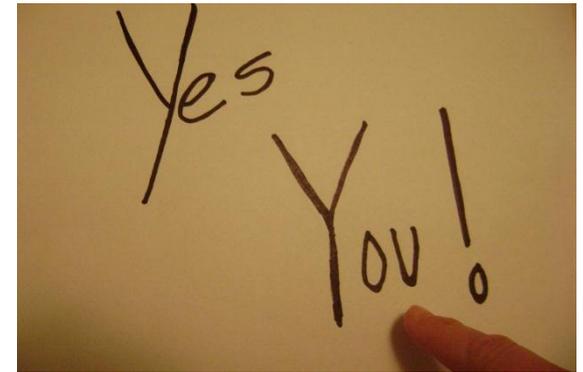
*We Answer the Call of Others...So They May Prevail*



# Target



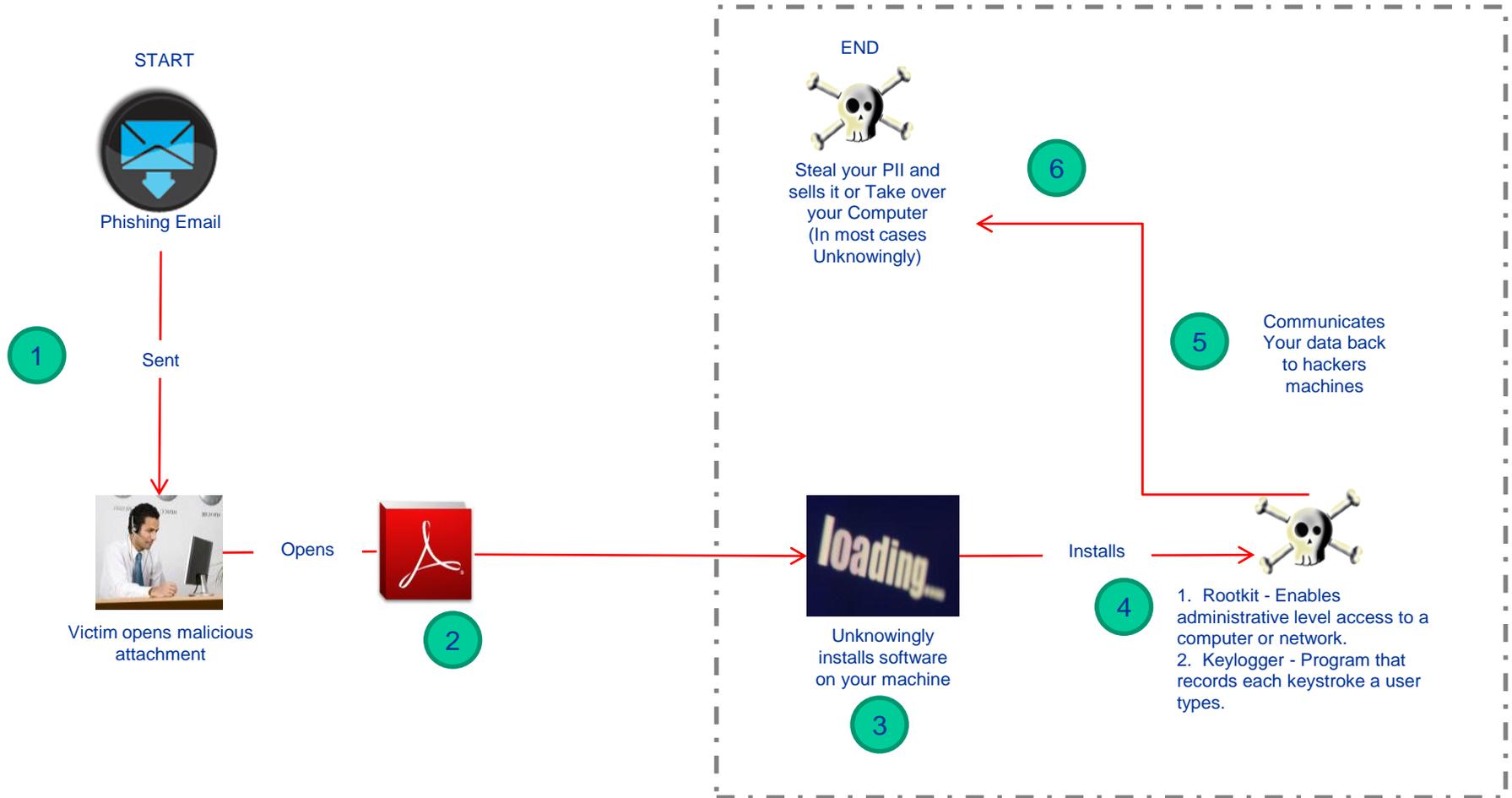
**YOU ARE A  
TARGET!**



*We Answer the Call of Others...So They May Prevail*



# How Are they doing it?



*We Answer the Call of Others...So They May Prevail*



# Phishing Indicators



## **Generic greeting:**

To save time, Internet criminals use generic names like "First Generic Bank Customer" so they don't have to type all recipients' names out and send emails one-by-one. If you don't see your name, be suspicious.

From: First Generic Bank <accounts@firstgenericbank.com>  
Subject: Please update your account information  
Date: Sep 12, 2006 3:23 PM PST

---

Dear First Generic Bank user,

As a courtesy to our valued customers, First Generic Bank conducts regular account information verification processes. During the most recent process, we found that we could not verify your information.

In order to ensure your account information is not made vulnerable, please visit <http://www.firstgenericbank.com.account-updateinfo.com>.

Please click on the above link to our Web site and confirm or update your account information. If you do not do this within 48 hours of receipt of this e-mail, you will not be able to use your First Generic Bank account for 30 days. This is an extra precaution we take to ensure your account remains secure.

Sincerely,  
First Generic Bank

## **Requests personal information:**

The point of sending phishing email is to trick you into providing your personal information. If you receive an email requesting your personal information, it is probably a phishing attempt.

## **Forged link:**

Roll your mouse over the link and see if it matches what appears in the email. If there is a discrepancy, don't click on the link. Also, websites where it is safe to enter personal information begin with "https" — the "s" stands for secure. If you don't see "https" do not proceed.

## **Sense of urgency:**

Internet criminals want you to provide your personal information now. They do this by making you think something has happened that requires you to act fast. The faster they get your information, the faster they can move on to another victim.



# Protect Yourself

**Trust Center**

Trusted Publishers

Add-ins

Privacy Options

**E-mail Security**

Attachment Handling

Automatic Download

Macro Security

Programmatic Access

**Encrypted e-mail**

- Encrypt contents and attachments for outgoing messages
- Add digital signature to outgoing messages
- Send clear text signed message when sending signed message
- Request S/MIME receipt for all S/MIME signed messages

Default Setting: Certificates [Settings...]

**Digital IDs (Certificates)**

Digital IDs or Certificates are documents that allow you to prove your identity.

[Publish to GAL...] [Import/Export...] [Get a Digital ID...]

**Read as Plain Text**

Read all standard mail in plain text

1. Encrypt sensitive information
2. Add digital signatures to outgoing messages
3. Implement READ Methodology
4. Ensure email is digitally signed before opening attachments or clicking links

Win a HDSE Plasma HDTV - Message (Plain Text)

This message was converted to plain text.

From: 375 Para Support Squadron [mailto:375PS@af.mil]  
To: [mailto:375PS@af.mil]  
Cc: [mailto:375PS@af.mil]  
Subject: Win a HDSE Plasma HDTV

ARE YOU READY FOR SOME FOOTBALL TV GIVEAWAY? <<http://148.125.6.31/news/rfllogo.asp>>

In celebration of the new football season, we are giving away a Samsung 63" 1680p plasma HDTVs. Click on the TV below to enter.

<<http://148.125.6.31/>>

Rules: All eligible entries will have an equal chance of winning one (1) of six (6) available Samsung 63" plasma HDTVs. Only one entry per person. Winners will be chosen by drawing of the last day of Are You Ready for Some Football TV Giveaway event, October 15, 2009. Winners will be announced October 30, 2009 via email.

Eligibility: As such it is open to active duty, guard and reserve members of the armed forces and their families; DoD civilians; retired military members and their family members; honorably discharged veterans with 100% service-connected disability and their family members; and former and/or surviving military spouses and their family members.



**READ Methodology**

Is Email :

- R = Relevant?
- E = Expected?
- A = Addressed Properly?
- D = Digitally Signed?

*We Answer the Call of Others...So They May Prevail*



# If you suspect “Phishing”



- 
- **Do not click on ANYTHING or open any attachments**
  - **Notify your Information System Assurance Officer (IAO) or Wing Information Assurance Office ASAP**