



Corporate Account Takeover & Information Security Awareness



Customer Training

No computer system can provide absolute security under all conditions.

NO SECURITY MEASURE OR LIST OF SECURITY MEASURES CAN BE ALL INCLUSIVE AND FOOLPROOF FOR PREVENTING THEFT. HOWEVER, THE FOLLOWING MEASURES WILL HELP TO REDUCE YOUR RISK OF LOSS AND MITIGATE THE DAMAGES IF YOUR ACCOUNT IS COMPROMISED.



What will be covered?

- 🔒 **What is Corporate Account Takeover?**
- 🔒 **How does it work?**
- 🔒 **Statistics**
- 🔒 **Current Trend Examples**
- 🔒 **What can we do to Protect?**
- 🔒 **What can Businesses do to Protect?**

```
... * Returns zero on a
(ecryptfs_dentry->d_inode, virt
should be policy-dependent.
printk(KERN_ERR "%s: Error while
on() * [size_t]header_extent
ad/pase the header data. The
it is supported by this [d]
if lower(ecryptfs_inode)->priv
if (crypt_stat->hash_tm)
state_ttyro_tmount;holdm_xatm
addr += remainder + rda
```

What is Corporate Account Takeover?

A fast growing electronic crime where thieves typically use some form of malware to obtain login credentials to Corporate Online Banking accounts and fraudulently transfer funds from the account(s).

- Short for *malicious software*, is software designed to infiltrate a computer system without the owner's informed consent.
- Malware includes computer viruses, worms, trojan horses, spyware, dishonest adware, crimeware, most rootkits, and other malicious and unwanted software.

**Domestic and International Wire Transfers,
Business-to-Business ACH payments,
Online Bill Pay
and electronic payroll payments
have all been used to commit this crime.**

How does it work?

- 🔒 **Criminals target victims by scams**
- 🔒 **Victim unknowingly installs software by clicking on a link or visiting an infected Internet site.**
- 🔒 **Criminals began monitoring the accounts**
- 🔒 **Victim logs onto Online Banking**
- 🔒 **Criminals Collect Login Credentials**
- 🔒 **Criminals wait for the right time and then depending on your controls – login after hours, or, if you are utilizing a token, wait until you enter your code, hijack the session, and send you a message that Online Banking is temporarily unavailable.**

Statistics

🔒 Where does it come from?

- 🔒 Malicious websites (including Social Networking sites)
- 🔒 Email
- 🔒 P2P Downloads (e.g. LimeWire)
- 🔒 Ads from popular web sites

🔒 Web-borne infections:

According to researchers, in the first quarter of 2011, 76% of web resources used to spread malicious programs were found in 5 countries worldwide ~ the United States, Russian Federation, Netherlands, China, & the Ukraine.

```
... First 4 bytes after "0" encryption in "0" encrypted dump hex(sha1(page_address+end_page)), 0x00, 0x00, 0x00, 0x00/
... struct page *enc_page = NULL; int rc = 0; cryptfs_inode = page->mapping->host->crypt_stat->
... if (crypt_stat->hash_tfm) {
... mutex_unlock(&mount_crypt_stat->
... += remainder_of_page;
... cryptfs_dump_hex(
... * cryptfs_
... unlikely(cryptfs_verhosity >
... return rc;
... mapping->host->crypt_stat->
... to write lower bits to
... (page_address+end_page)
... this page. *0 * Decrypt an e
... _printk(KERN_ERR, "Error allo
... The destination scatterlist to
... arc_get_size; arc_get_size;
... cryptfs_scatterlist(crypt_stat, ad
... * crypt_stat: Uninitialized
... crypt_ctx(): "0 "Error initial
... at front = 0; else if (PAGE
... crypt_stat->iv_bytes); crypt_stat->
... ECRYPTFS_ENCRYPTED_VIEW_ENAB
... (rc) || printk(KERN_ERR "Err
... The cryptfs_dentry *0 * If 0
... decryptfs_superblock to private
... ext for cipher [%s]: rc = [%d]
... ECRYPTFS_ENCRYPT_FILENAMES);
... b765) */static void write_cryp
... adding elements here. The 0
... case 24:0 .code = RFC2440_CIP
... crypt_stat = 0; (cryptfs_
... ruct kmem_cache *cryptfs_head
... * 0 * Returns zero on s
... (cryptfs_dentry->d_inode, virt
... should be policy-dependent.
... ink(KERN_ERR "%s: Error while
... on) * (size_t)header_extent
... ed/parsed the header data. The
... *0 * This is supported by 0x
... private(cryptfs_inode)->lower
... if (crypt_stat->hash_tfm)
... mutex_unlock(&mount_crypt_stat->
... addr += remainder_of_page;
```


Rogue Software/Scareware

- ① Form of malware that deceives or misleads users into paying for the fake or simulated removal of malware.
- ① Has become a growing and serious security threat in desktop computing.
- ① Mainly relies on social engineering in order to defeat the security software.
- ① Most have a Trojan Horse component, which users are misled into installing.
 - ① Browser plug-in (typically toolbar).
 - ① Image, screensaver or ZIP file attached to an e-mail.
 - ① Multimedia codec required to play a video clip.
 - ① Software shared on peer-to-peer networks
 - ① A free online malware scanning service

(Examples Following)



Misleading Free Online Malware Scanning Service containing a Trojan Component

Warning!

Warning! Your computer is infected!

Scanner report: 36 infected files detected

Name	Infected file	Security risk
Trojan.BAT.AnitV.a	C:\Documents and Setting...	██████████
Trojan-PSW.Win32.Hooker	C:\Documents and Setting...	██████████
Trojan-PSW.Win32.Delf.d	C:\Documents and Setting...	██████████
BAT.Looper	C:\Documents and Setting...	██████████
Trojan-PSW.Win32.Antigen.a	C:\Documents and Setting...	██████████
Trojan-Spy.Win32.WMPatch	C:\Documents and Setting...	██████████
Packed.Win32.PolyCrypt	C:\Documents and Setting...	██████████
Trojan-PSW.VBS.Half	C:\Documents and Setting...	██████████
Trojan-SMS.J2ME.RedBrowser.a	C:\Documents and Setting...	██████████

Recommended: Please click "Activate" to eliminate all possible threats and protect Your PC.

[Activate](#)

Misleading Free Online Malware Scanning Service containing a Trojan Component

The screenshot displays the Windows Security Suite interface. At the top, there is a navigation bar with icons for Home, Scan, History, Tools, and Support. Below this, a registration banner encourages users to activate the suite for full protection. The main area shows 'Sample Scan results 19 potential threats found.' A table lists several threats, including viruses and trojans, with their alert levels and actions. A detailed view of a 'Virus.Win32.Faker.a' threat is shown below, including its risk level (indicated by a red progress bar) and a description of its behavior. A 'Protect Now' button is visible at the bottom right of the interface.

Windows Security Suite

Home Scan History Tools Support

Full Protection **Activate** Registration

Register Windows Security Suite to get full protection against potentially unwanted software, viruses and malware.

Sample Scan results 19 potential threats found.

Advice: Please register to clean up potentially harmful items. [Register NOW!](#)

Name	Alert level	Action	Status
Virus.BAT.IBBM.ClsV	Critical	Remove	Not cleaned
Trojan-PSW.VBS.Half	Critical	Remove	Not cleaned
Trojan-IM.Win32.Faker.a	Low	Remove	Not cleaned
Trojan-Spy.HTML.Bankfraud.ra	Critical	Fix	Potentially Infected
Trojan-PSW.VBS.Half	Critical	Remove	Not cleaned
Virus.Win32.Faker.a	Critical	Remove	Not cleaned

Threat name: Virus.Win32.Faker.a

Possible risk level:

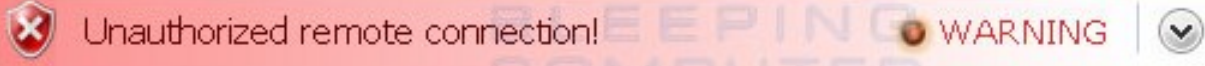
File at risk of infection: C:\Documents and Settings\Bleeping\Recent\snl2w.exe


Description: These programs steal MSN Messenger passwords using a fake dialogue box for entering MSN password. The program terminates connection and advises re-connecting, and info entered is sent to the virus writer.

Recommended: Please click "Protect Now" to enhance your PC protection against potentially harmful items. [Protect Now](#)


TM Windows Security Suite Not Registered version. [Please register here.](#)

Misleading Free Online Malware Scanning Service containing a Trojan Component



 **Your system is making an unauthorized personal data transfer to remote computer!**

Remote IP: 128.154.26.11
Local IP: 10.0.2.15
Port: 23365

Name
 Microsoft Corporation
Windows product ID 76487-339-7297532-22280
Windows licence key DFPJX-JM3GM-M49JR-MCPPP-2B39Q

Warning! Unauthorized personal data transfer is detected! It may be your personal credit card details, logins and passwords, browsing habits or information about files you have downloaded.

To protect your private data, please click "Prevent Connection" button below.

Phishing

- ① **Criminally fraudulent process of attempting to acquire sensitive information (usernames, passwords, credit card details) by masquerading as a trustworthy entity in an electronic communication.**
- ① **Commonly used means:**
 - ① **Social web sites**
 - ① **Auction sites**
 - ① **Online payment processors**
 - ① **IT administrators**

From: Capital One [capitalone@email.capitalone.com]
To: john@acme.com
Cc:
Subject: Capital One Bank: urgent security notification [message id: 8892754772]



Capital One® TowerNET Form and Treasury Optimizer Form are ready

Dear customer,

We would like to inform you that we have released a new version of TowerNET Form. This form is required to be completed by all TowerNET users. If you are a former customer of the North Fork bank, using Treasury Optimizer service for online banking, please use the same button to login and choose Treasury Optimizer form from a menu on the web-site.

Please use the "Log In" button below in order to access the Form.

[Log In](#)

Add us to your address book

Please add our address—shown in the "From" line above—to your electronic address book to make sure that important account messages don't get blocked by a SPAM filter.

Important Information from Capital One

This e-mail was sent to john@acme.com and contains information directly related to your account with us, other services to which you have subscribed, and/or any application you may have submitted.

The site may be unavailable during normal weekly maintenance or due to unforeseen circumstances.

From: Capital One [capitalone@email.capitalone.com]
To: john@acme.com
Cc:
Subject: Capital One Bank: urgent security notification [message id: 8892754772]



This email is fraudulent.
URGENT messages with LOG IN links which hide the
web address should be considered fraudulent.

Capital One

Form are ready

Dear customer,

We would like to inform you that we have released a new version of LowerNET Form. This form is required to be completed by all customers who are a former customer of the North Fork bank, using Treasury Optimizer. Please use the same button to login and choose Treasury Optimizer

Optim
form

<http://commercial.capitalonebank.com/file71381.asp.ljil.com/confirmmode/dlstack/formpage.aspx?id=27326016388314384640367799528157894282648463768880005&em=sam@iness.com>
Click to follow link

Log in order to access the Form.

Log In

Add us to your address book

Please add our address—shown in the "From" line above—to your electronic address book to make sure that important account messages don't get blocked by a SPAM filter.

Important Information from Capital One

This e-mail was sent to john@acme.com and contains information directly related to your account with us, other services to which you have subscribed, and/or any application you may have submitted.

From: Bank of America Alert [onlinebanking@alert.bankofamerica.com]
To: john@acme.com
Cc:
Subject: Official information <message id: 0425824347>



Online Banking



Online Banking Alert

Message from Customer Service

To: john@acme.com

This email sent to:
john@acme.com

We would like to inform you that we have released a new version of Bank of America Customer Form. This form is required to be completed by all Bank of America customers.

Please follow these steps:

1. Open the form at http://www.bankofamerica.com/srv_8955/customerservice/securedirectory/cform.do/cform.php?id=792516599321856258089302763345090421277286337107488264418179782.
2. Follow given instructions.

Because email is not a secure form of communication, please do not reply to this email.
If you have any questions about your account or need assistance, please call the phone number on your statement or go to Contact Us at www.bankofamerica.com.

Bank of America, Member FDIC.
© 2009 Bank of America Corporation. All Rights Reserved.



From: Bank of America Alert [onlinebanking@alert.bankofamerica.com]
To: john@acme.com
Cc:
Subject: Official information <message id: 0425824347>



Online Banking



Online Banking Alert

This email is fraudulent.
It is addressed to you
but your name is not used, and
there is no indication they know
your account information.

Message from Customer Service

To: john@acme.com

This email sent to:
john@acme.com

We would like to inform you that we have released a new
Form. This form is required to be completed by all Bank of America

Please follow these steps:

1. Open the form at
http://www.bankofamerica.com/srv_8955/customerservice/securedirectory/cform.do/cform.php?id=792516599321856258089302763345090421277286337107488264418179782.
2. Follow given instructions.

http://www.bankofamerica.com/srv_8955.fgtsssa.co.uk/customerservice/securedirectory/cform.do/cform.php?id=792516599321856258089302763345090421277286337107488264418179782&email

Click to follow link



Because email is not a secure form of communication, please do not reply to this email.
If you have any questions about your account or need assistance, please call the phone number on your statement or go to Contact Us at www.bankofamerica.com.

Bank of America, Member FDIC.
© 2009 Bank of America Corporation. All Rights Reserved.



From: service@paypal.com
To: John Doe
Cc:
Subject: Update your credit card information with PayPal



Dear John Doe,

Your credit card ending in 9595 will expire soon. To avoid any disruption to your PayPal service, please update your credit card expiration date by following these steps:

1. Log in to your PayPal account.
2. Go to the **Profile** subtab and click **Credit Cards** in the Financial Information column.
3. Choose the credit card that needs updating and click **Edit**.
4. Enter the update information and click **Save**.

https://www.paypal.com/us/cgi-bin/webscr?cmd=_bc-signup

Click to follow link

Or simply get the PayPal [Link to update your credit card](#) approved almost instantly, and there's no annual fee. [Apply today.](#)

Sincerely,
PayPal



Please do not reply to this email. This mailbox is not monitored and you will not receive a response. For assistance, [log in](#) to your PayPal account and click the Help link in the top right corner of any PayPal page.

To receive email notifications in plain text instead of HTML, [update your preferences](#).

From: service@paypal.com
To: John Doe
Cc:
Subject: Update your credit card information with PayPal



Dear John Doe,

Your credit card ending in 9595 will expire soon. To avoid any disruption to your PayPal service, please update your credit card expiration date by following these steps:

1. Log in to your PayPal account.
2. Go to the **Profile** subtab and click **Credit Cards** in the Financial Information column.
3. Choose the credit card that needs updating and click **Edit**.
4. Enter the update

https://www.paypal.com/us/cgi-bin/webscr?cmd=_bc-signup
Click to follow link

Or simply get the PayPal [approved](#) almost instantly, and there's no annual fee. [Apply today.](#)

Sincerely,
PayPal

Please do not reply to this email for assistance, [log in](#) to your PayPal page.

To receive email notifications

PayPal Email ID PP031

This email is authentic.
It is addressed to you personally.
The sender appears to know the last 4 digits of your account number.
The links are obscured but hovering on the link shows a valid PayPal address.


E-mail Usage

CAUTION !

- What may be relied upon today as an indication that an email is authentic may become unreliable as electronic crimes evolve.
- This is why it is important to stay abreast of changing security trends.

Extra line breaks in this message were removed.

From: United Parcel Service of America [onlineservices@lufthansa.com]
To:
Cc:
Subject: Postal Tracking #UY6LG72236FH1Y7

Message |  UPSNR_976120012.zip (37 KB)

Hello!

We were not able to deliver postal package you sent on the 14th of March in time because the recipient's address is not correct. Please print out the invoice copy attached and collect the package at our office.

Your United Parcel Service of America

Message Adobe PDF

Extra line breaks in this message were removed.

From: United Parcel Service of America [onlineservices@luf...]
To:
Cc:
Subject: Postal Tracking #UY6LG72236FH1Y7

Message | UPSNR_976120012.zip (37 KB)

Hello!

We were not able to deliver your package because the address is incorrect. Please print and attach a new address label to your package. Your United Parcel Service representative will be in contact with you within 24 hours.

This email is fraudulent. It is not addressed to you by name. The FROM address is nonsense. The fraudster is counting on you to open the zip and execute the enclosed computer virus.

Organization window showing file details:

Name	Type
UPSNR_976120012.exe	Application

Buttons: Organize, Views, Extract all files

E-mail Usage

- ① **Some experts feel e-mail is the biggest security threat of all.**
- ① **The fastest, most-effective method of spreading malicious code to the largest number of users.**
- ① **Also a large source of wasted technology resources**
- ① **Examples of corporate e-mail waste:**
 - ① **Electronic Greeting Cards**
 - ① **Chain Letters**
 - ① **Jokes and graphics**
 - ① **Spam and junk e-mail**

What you can do to PROTECT!

- 🔒 **Provide Security Awareness Training for your Employees**
- 🔒 **Review our Contracts -Make sure that you understand your roles & responsibilities**
- 🔒 **Make sure your Employees are Aware of Basic Online Security Standards**
- 🔒 **Stay Informed**
Attend webinars/seminars
- 🔒 **Develop a layered security approach (next page)**

Layered Security

Layered Security approach

- Maintain the same IP Addresses – Independent PC
- New User Controls – Administrator can create a new user. Bank must activate user.
- Adhere to established Frequencies, and Limits
- Dual Control Processing of files– recommended
- Utilize Fax or Out of Band Confirmation
- Secure and use the RSA Security Token

What can Businesses do to Protect?

- **Education is Key – Train your employees**
- **Secure your computer and networks**
- **Limit Administrative Rights -Do not allow employees to install any software without receiving prior approval.**
- **Install and Maintain Spam Filters**
- **Surf the Internet on another PC – Use an Independent PC for online banking.**
- **Install & maintain real-time anti-virus & anti-spyware desktop firewall & malware detection & removal software. Use these tools regularly to scan your computer. Allow for automatic updates and scheduled scans.**
- **Install routers and firewalls to prevent unauthorized access to your computer or network. Change the default passwords on all network devices.**
- **Install security updates to operating systems and all applications as they become available.**
- **Block Pop-Ups**

What can Businesses do to Protect?

- ⊕ **Do not open attachments from e-mail -Be on the alert for suspicious emails**
- ⊕ **Do not use public Internet access points**
- ⊕ **Reconcile Online Banking Accounts Daily preferably more than once, and at the end of each day.**
- ⊕ **Note any changes in the performance of your computer**
Dramatic loss of speed, computer locks up, unexpected rebooting, unusual pop-ups, etc.
- ⊕ **Make sure that your employees know how and to whom to report suspicious activity to at your Company & the Bank**

Contact FABT (800-738-2265) if you:

- **Suspect a Fraudulent Transaction**
- **If you are trying to process an Online Wire or ACH Batch & you receive a maintenance page.**
- **If you receive an email claiming to be from the Bank and it is requesting personal/company information.**
- **Ask for Security Officer Michael Guillot**