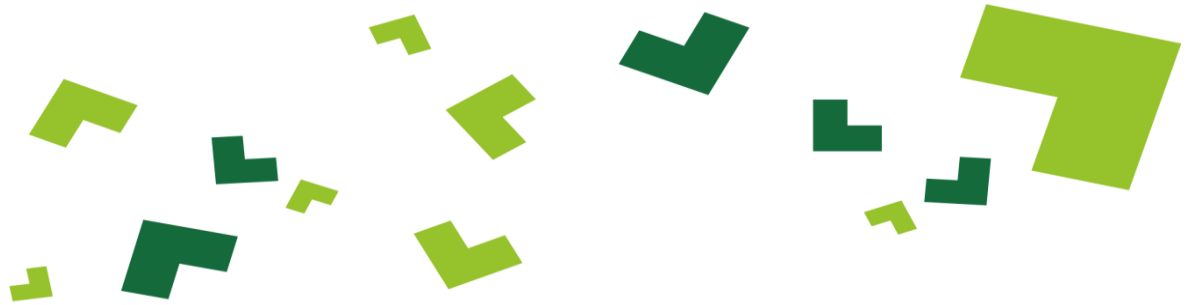




SMARTCOM



Smartcom Security awareness training - 18.01.2017

Mircho Mirchev



What is the most secure device?

The only secure computer is one that's unplugged, locked in a safe, and buried 20 feet under the ground in a secret location... and I'm not even too sure about that one.

—Dennis Hughes, FBI

- Connect it to power - **you're exposed**
- Connect it network - **you're more exposed**
- Connect it Internet - **you're even more exposed**



IMPORTANCE OF SECURITY

- The Internet allows an attacker to attack from anywhere on the planet.
- Risks caused by poor security knowledge and practice:
 - Unauthorized access to information
 - Loss of access to information
 - Loss of information
 - Corruption of information
 - Theft of information
- According to www.SANS.org , the top vulnerabilities available for a cyber criminal are:
 - Web Browser
 - IM Clients
 - Web Applications
 - Excessive User Rights





The implications are non-trivial

- Loss of revenue
- Loss of business
- Fines, lawsuits, headlines
- Unbudgeted expenses
 - Breach costs currently estimated at around \$190 per record exposed*
 - 5,263 records = \$1 million hit



Trojan terminates escrow firm

- \$1.1 million wired to China and could not be retrieved
- Firm was closed by state law, now in receivership, 9 people out of a job
- So what's the best weapon for keeping that kind of Trojan code out of your company's system?





A well-trained workforce

- Knows not to click on suspicious links in email or social media
- Knows to report strange activity (e.g. the two-factor authentication not working)
- Knows to scan all incoming files for malware
 - Email, USB drives





Does training make a difference?

- Yes
- A significant percentage of problems can be averted, or their impact minimized, if more employees get better security training and education*

*A bunch of different studies in recent years



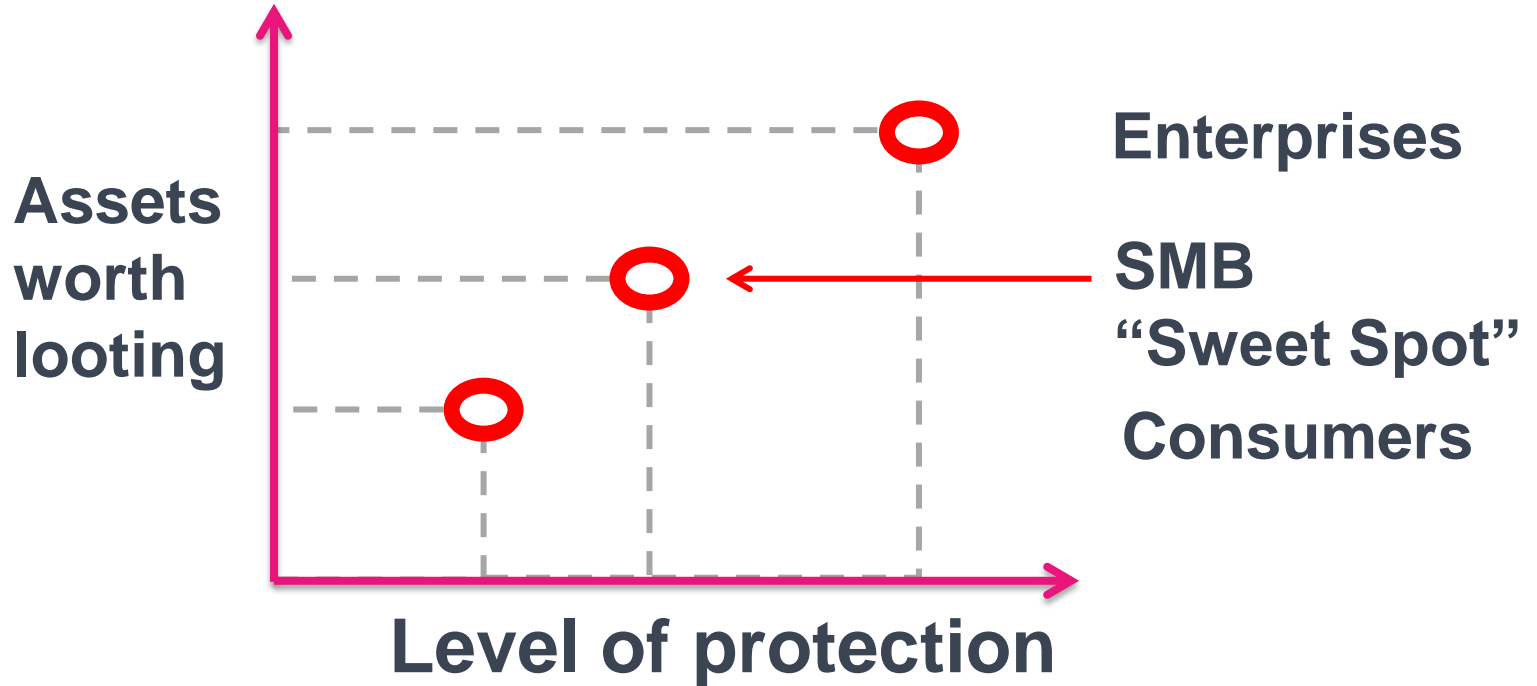
SECURITY VS SAFETY

Security: We must protect our computers and data in the same way that we secure the doors to our homes.

Safety: We must behave in ways that protect us against risks and threats that come with technology.



The **SMB Sweet Spot** for the cyber-criminally inclined



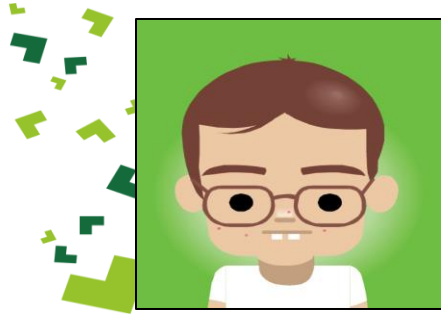


Purpose of this training is:

USER AWARENESS



Who is who



Cracker:
Computer-savvy programmer creates attack software

Script Kiddies:
Unsophisticated computer users who know how to execute programs



Criminals:
Create & sell bots -> spam
Sell credit card numbers,...



System Administrators
Some scripts are useful to protect networks...

Hacker Bulletin Board
SQL Injection
Buffer overflow
Password Crackers
Password Dictionaries

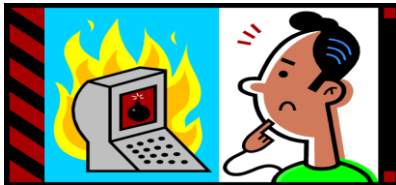
Successful attacks!
Crazyman broke into ...
CoolCat penetrated...

Malware package=\$1K-2K
1 M Email addresses = \$8
10,000 PCs = \$1000



LEADING THREATS

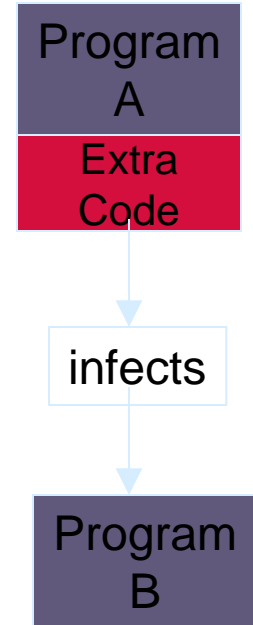
- Virus
- Worm
- Trojan Horse / Logic Bomb
- Social Engineering
- Rootkits
- Botnets / Zombies





VIRUS

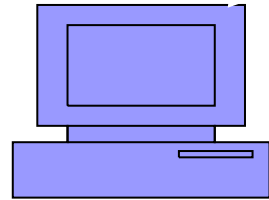
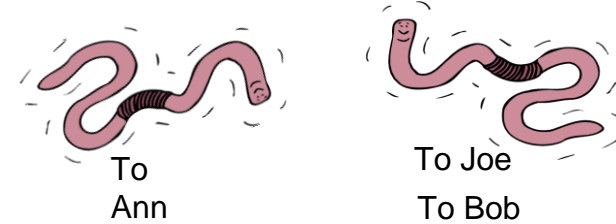
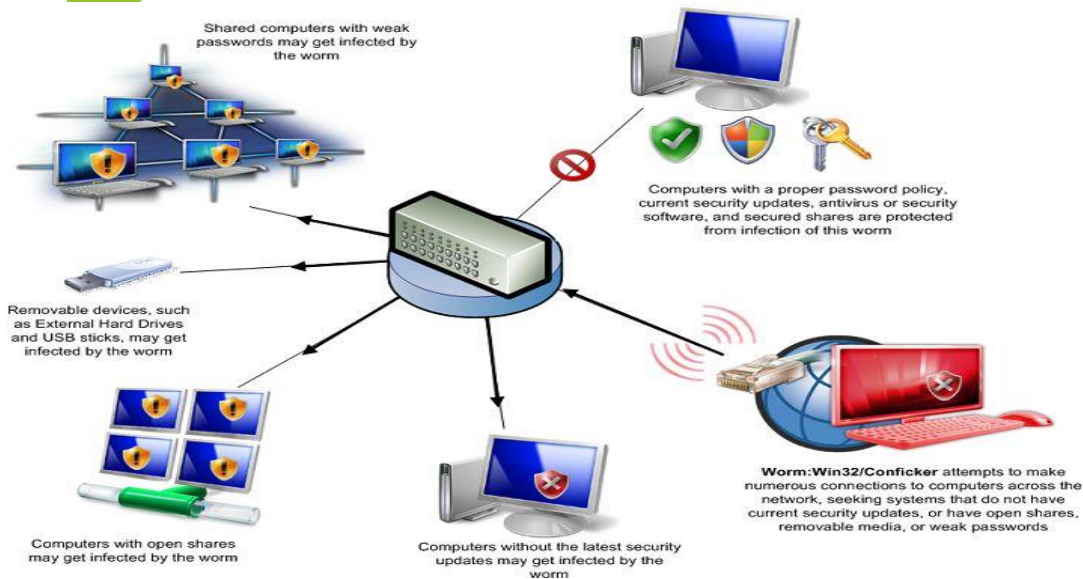
- A virus attaches itself to a program, file, or disk
- When the program is executed, the virus activates and replicates itself
- The virus may be benign or malignant but executes its payload at some point (often upon contact)
 - Viruses result in crashing of computers and loss of data.
- In order to recover/prevent virus/attacks:
 - Avoid potentially unreliable websites/emails
 - System Restore
 - Re-install operating system
 - Anti-virus (i.e. Avira, AVG, Norton)





WORM

- Independent program which replicates itself and sends copies from computer to computer across network connections. Upon arrival the worm may be activated to replicate.



Email List:
Joe@gmail.com
Ann@yahoo.com
Bob@uwp.edu



LOGIC BOMB / TROJAN HORSE

- **Logic Bomb:** Malware logic executes upon certain conditions. Program is often used for legitimate reasons.
 - Software which malfunctions if maintenance fee is not paid
 - Employee triggers a database erase when he is fired.
- **Trojan Horse:** Masquerades as beneficial program while quietly destroying data or damaging your system.
 - Download a game: Might be fun but has hidden part that emails your password file without you knowing.





SOCIAL ENGINEERING

- Social engineering manipulates people into performing actions or divulging confidential information. Similar to a confidence trick or simple fraud, the term applies to the use of deception to gain information, commit fraud, or access computer systems.

Phone Call:

This is John, the System Admin. What is your password?



Email:

ABC Bank has noticed a problem with your account...

In Person:

What ethnicity are you?
Your mother's maiden name?



and have some software patches

I have come to repair your machine...





PHISHING = FAKE EMAIL

- ◎ **Phishing:** a 'trustworthy entity' asks via e-mail for sensitive information such as SSN, credit card numbers, login IDs or passwords.





PHARMING = FAKE WEB PAGES



Dear valued customer of TrustedBank,

We have received notice that you have recently attempted to withdraw the following amount from your checking account while in another country: \$135.25.

If this information is not correct, someone unknown may have access to your account. As a safety measure, please visit our website via the link below to verify your personal information:

<http://www.trustedbank.com/general/custverifyinfo.asp>

Once you have done this, our fraud department will work to resolve this discrepancy. We are happy you have chosen us to do business with.

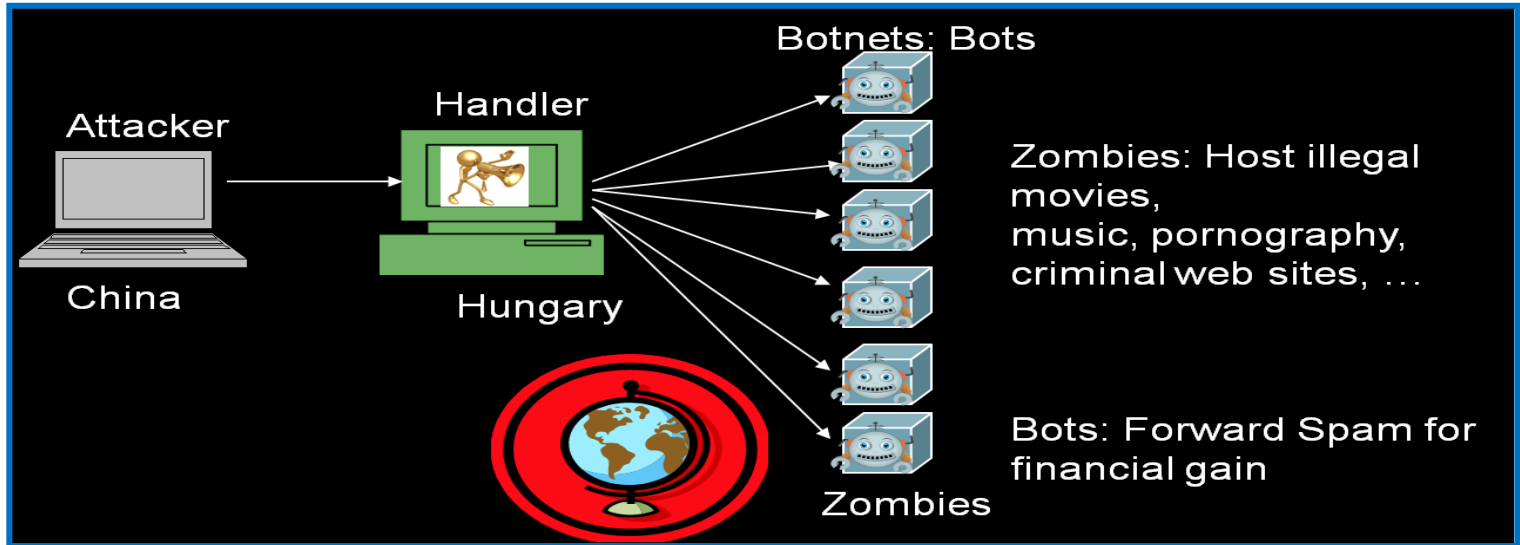
Thank you,
TrustedBank

Member FDIC © 2005 TrustedBank, Inc.

- The link provided in the e-mail leads to a fake webpage which collects important information and submits it to the owner.
- The fake web page looks like the real thing
 - Extracts account information

BOTNET

- A **botnet** is a large number of compromised computers that are used to create and send spam or viruses or flood a network with messages as a denial of service attack.
- The compromised computers are called **zombies**

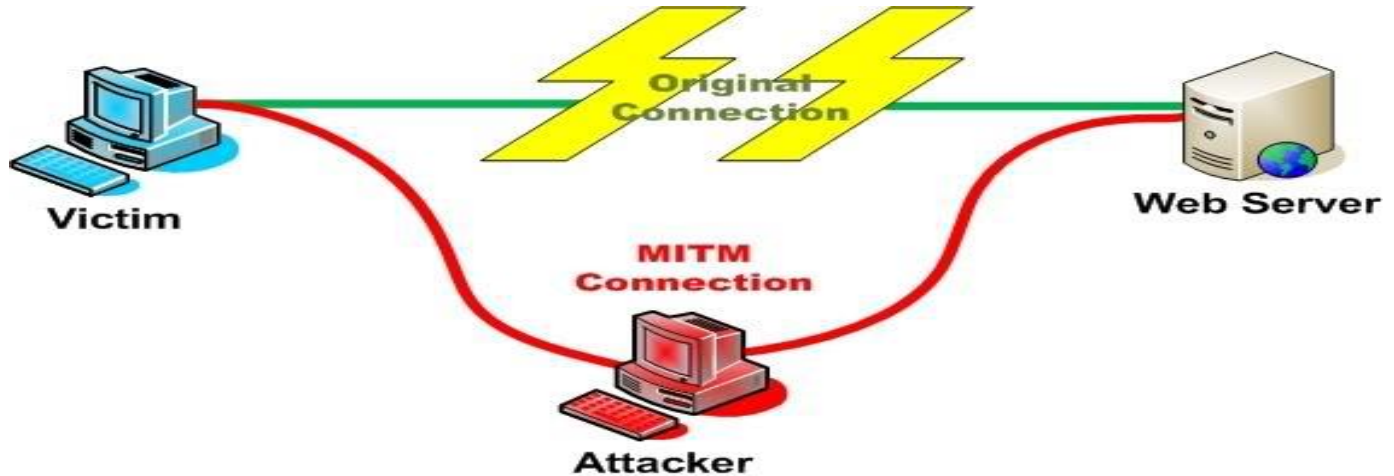




MAN IN THE MIDDLE ATTACK



- An attacker pretends to be your final destination on the network. If a person tries to connect to a specific WLAN access point or web server, an attacker can mislead him to his computer, pretending to be that access point or server.

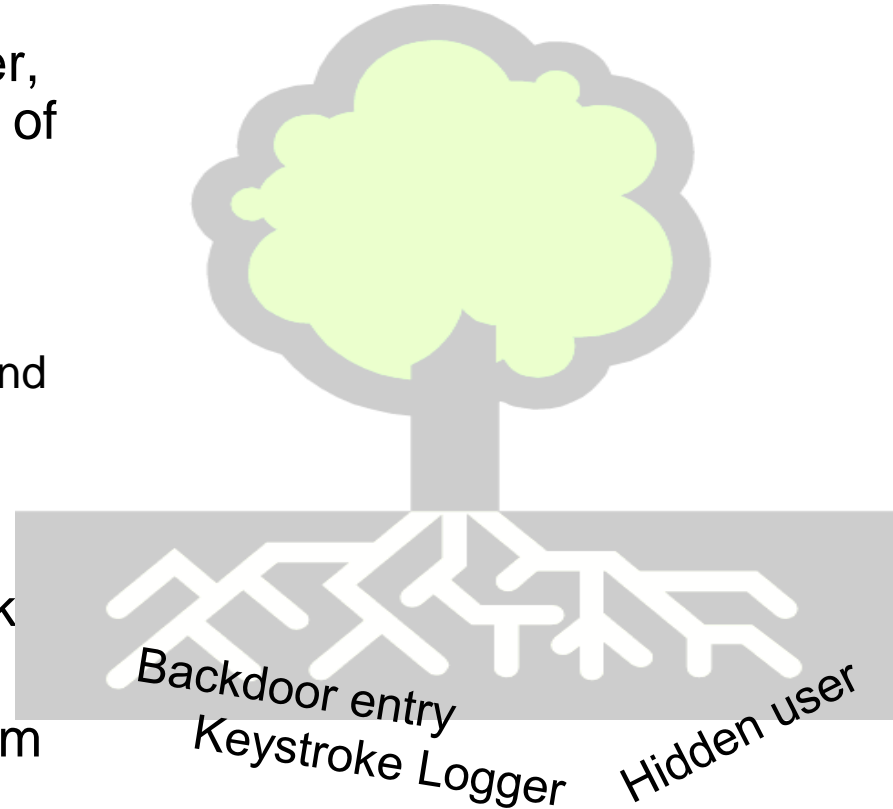




ROOTKIT



- Upon penetrating a computer, a hacker installs a collection of programs, called a **rootkit**.
- May enable:
 - Easy access for the hacker (and others)
 - Keystroke logger
- Eliminates evidence of break
- Modifies the operating system





PASSWORD CRACKING: DICTIONARY ATTACK & BRUTE FORCE

Pattern	Calculation	Result	Time to Guess (2.6×10^{18} /month)
Personal Info: interests, relatives		20	Manual 5 minutes
Social Engineering		1	Manual 2 minutes
American Dictionary		80,000	< 1 second
4 chars: lower case alpha	26^4	5×10^5	
8 chars: lower case alpha	26^8	2×10^{11}	
8 chars: alpha	52^8	5×10^{13}	
8 chars: alphanumeric	62^8	2×10^{14}	3.4 min.
8 chars alphanumeric +10	72^8	7×10^{14}	12 min.
8 chars: all keyboard	95^8	7×10^{15}	2 hours
12 chars: alphanumeric	62^{12}	3×10^{21}	96 years
12 chars: alphanumeric + 10	72^{12}	2×10^{22}	500 years
12 chars: all keyboard	95^{12}	5×10^{23}	
16 chars: alphanumeric	62^{16}	5×10^{28}	



RECOGNIZING A BREAK-IN OR COMPROMISE



- ◎ Symptoms:
 - Antivirus software detects a problem
 - Pop-ups suddenly appear (may sell security software)
 - Disk space disappears
 - Files or transactions appear that should not be there
 - System slows down to a crawl
 - Unusual messages, sounds, or displays on your monitor
 - Stolen laptop (1 in 10 stolen in laptop lifetime)
 - Your mouse moves by itself
 - Your computer shuts down and powers off by itself
 - Often not recognized



MALWARE DETECTION



- ◎ Spyware symptoms:
 - Change to your browser homepage/start page
 - Ending up on a strange site when conducting a search
 - System-based firewall is turned off automatically
 - Lots of network activity while not particularly active
 - Excessive pop-up windows
 - New icons, programs, favorites which you did not add
 - Frequent firewall alerts about unknown programs trying to access the Internet
 - Bad/slow system performance



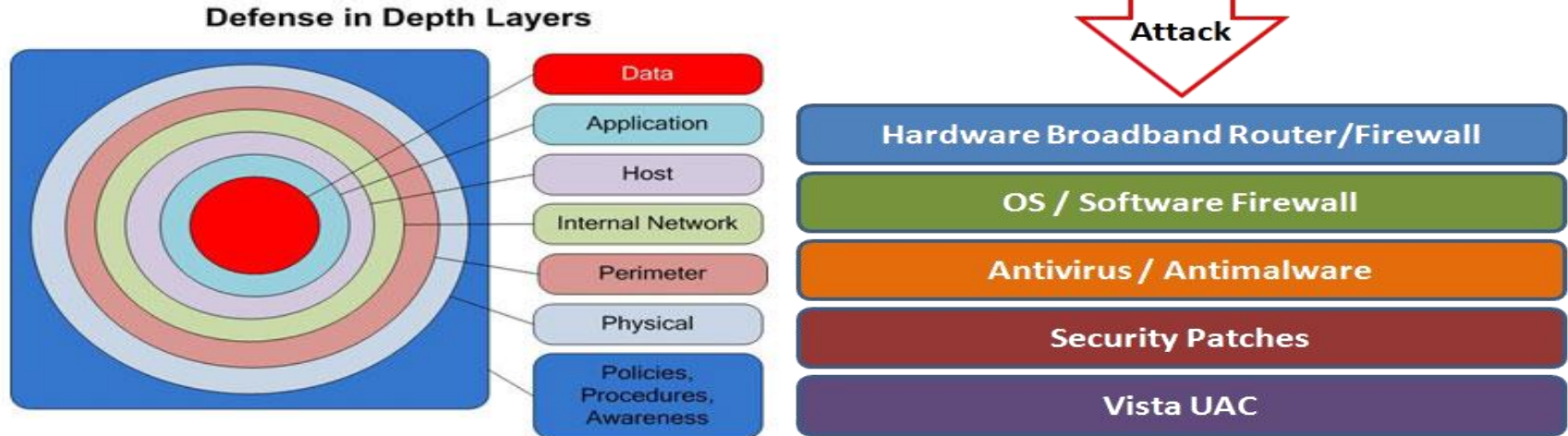
(with examples)

SAFE & SECURE USER PRACTICES



SECURITY: DEFENSE IN DEPTH

Defense in depth uses multiple layers of defense to address technical, personnel and operational issues.

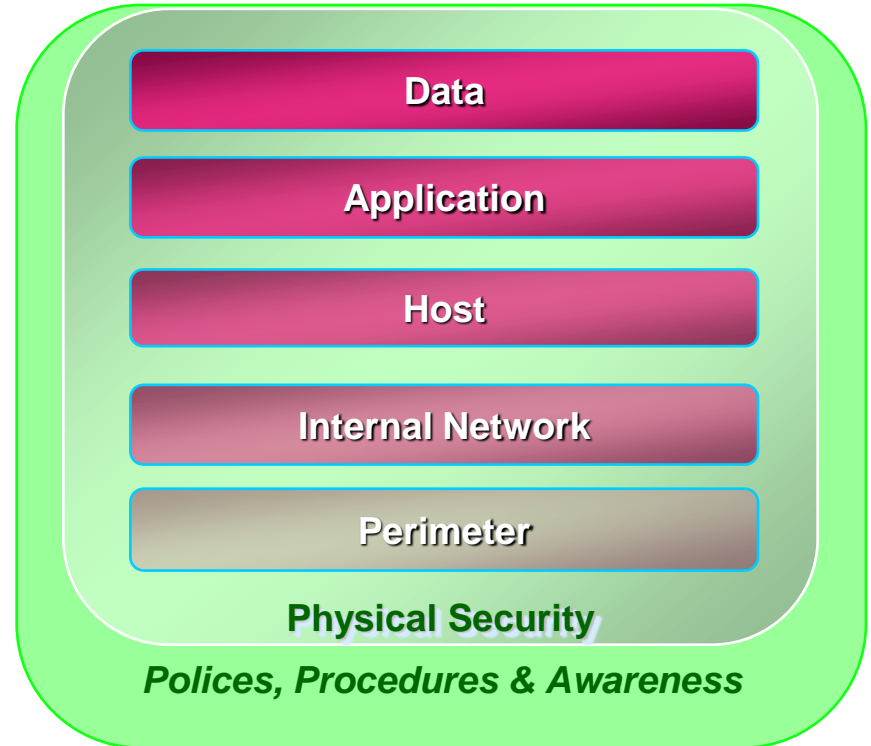




Positioning End User Security Awareness for Business



- End User Security and Awareness programs reside in the Policies, Procedures, and Awareness layer of the Defense in Depth security model.
- User security awareness can affect every aspect of an organization's security profile.
- User awareness is a significant part of a comprehensive security profile because many attack types rely on human intervention to succeed.

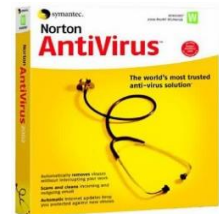




ANTI-VIRUS & ANTI-SPYWARE



- Anti-virus software detects malware and can destroy it before any damage is done
- Install and maintain anti-virus and anti-spyware software
- Be sure to keep anti-virus software updated
- Many free and pay options exist

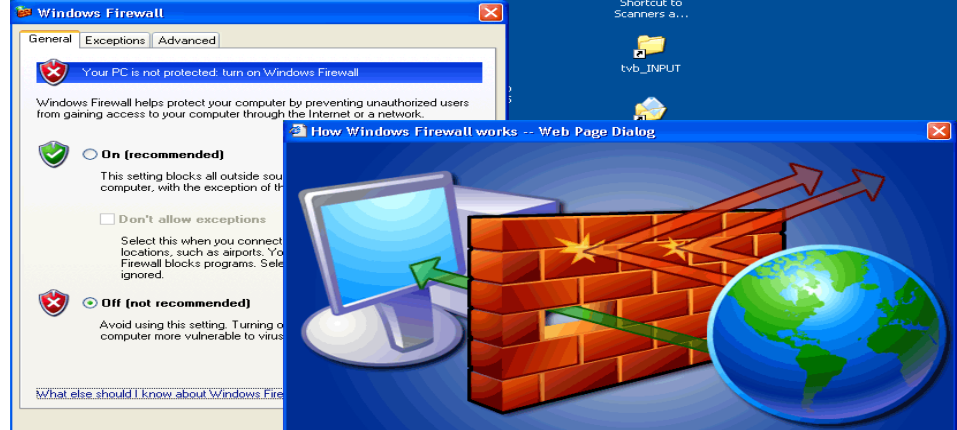




FIREWALL



- A firewall acts as a wall between your computer/private network and the internet. Hackers may use the internet to find, use, and install applications on your computer. A firewall prevents hacker connections from entering your computer.
- Filters packets that enter or leave your computer

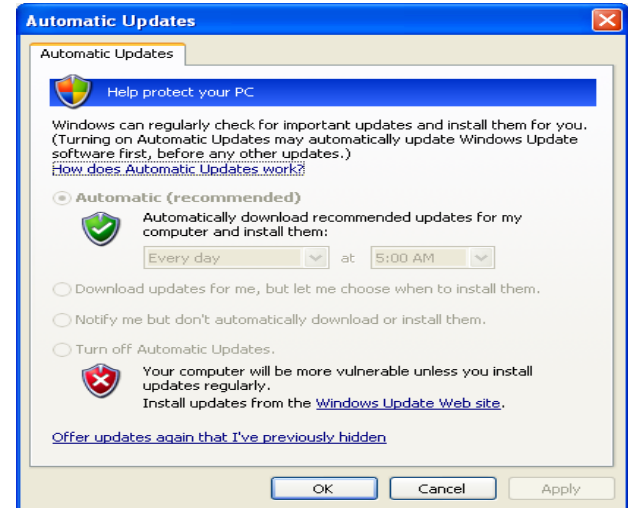
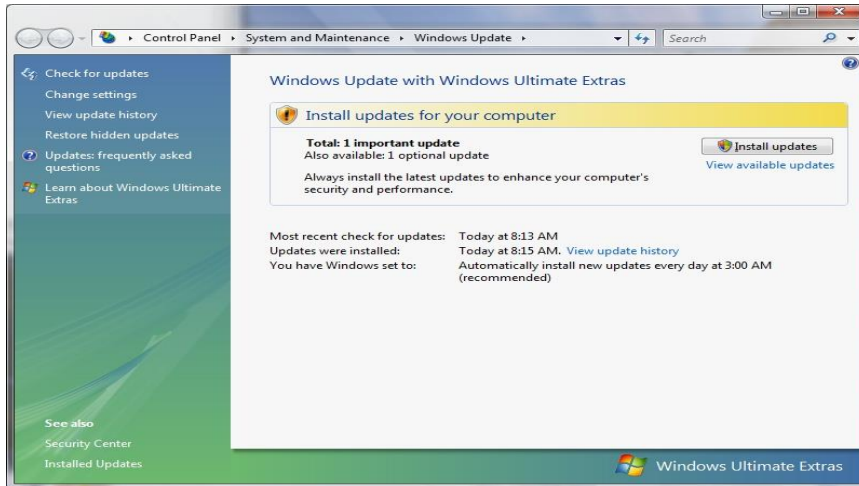




PROTECT YOUR OPERATING SYSTEM

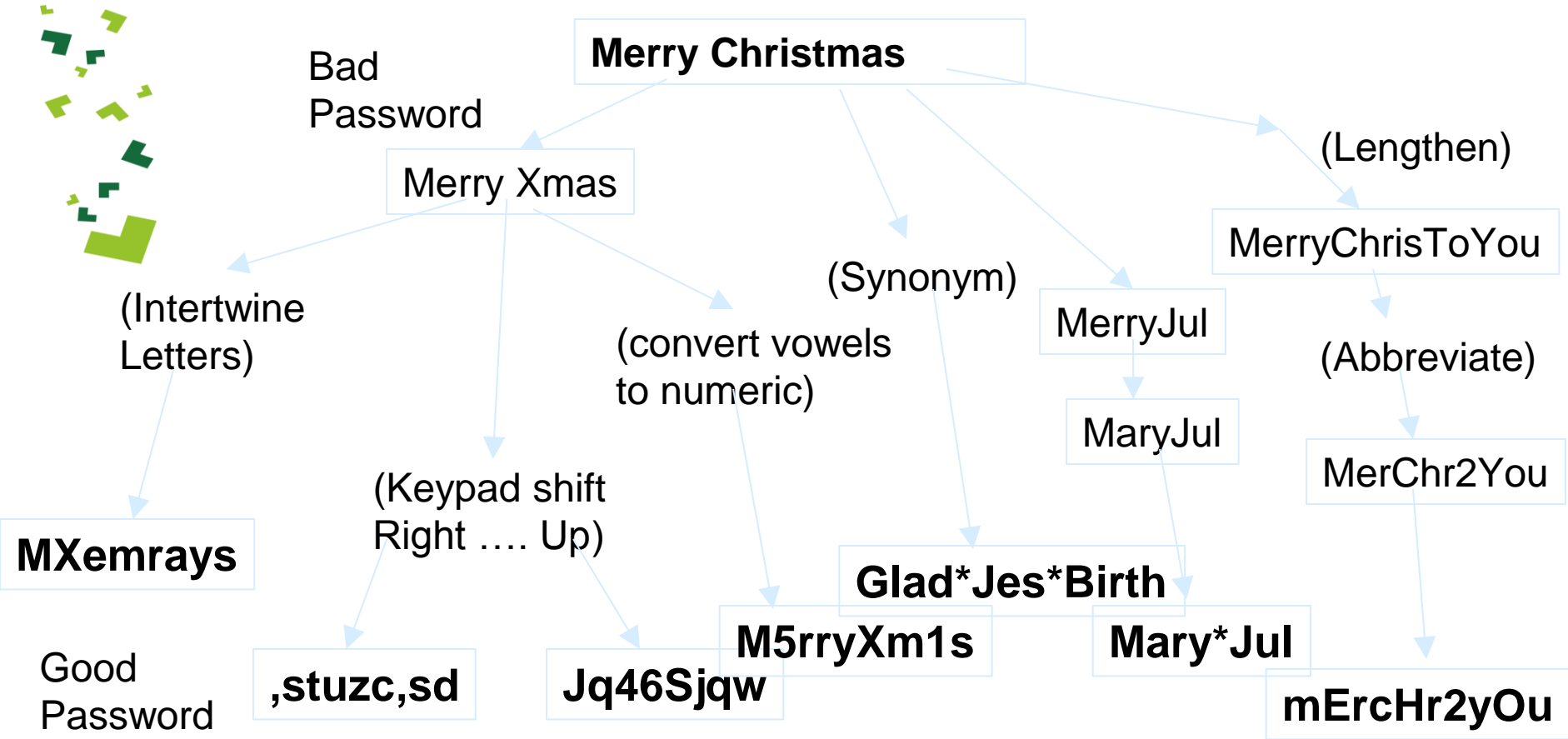


- Microsoft regularly issues patches or updates to solve security problems in their software. If these are not applied, it leaves your computer vulnerable to hackers.
- The Windows Update feature built into Windows can be set up to automatically download and install updates.
- Avoid logging in as administrator





CREATING A GOOD PASSWORD (1/2)





CREATING A GOOD PASSWORD (2/2)

Combine 2 unrelated words

Mail + phone = m@!lf0n3

Abbreviate a phrase

My favorite color is blue=
Mfciblue

Music lyric

Happy birthday to you, happy birthday to you, happy birthday dear John, happy birthday to you.

hb2uhb2uhbdJhb2u





PASSWORD RECOMMENDATIONS

- Never use 'admin' or 'root' or 'administrator' as a login for the admin
- A good password is:
 - **private:** it is used and known by one person only
 - **secret:** it does not appear in clear text in any file or program or on a piece of paper pinned to the terminal
 - **easily remembered:** so there is no need to write it down
 - **at least 8 characters, complex:** a mixture of at least 3 of the following: upper case letters, lower case letters, digits and punctuation
 - **not guessable** by any program in a reasonable time, for instance less than one week.
 - **changed regularly:** a good change policy is every 3 months
- Beware that someone may see you typing it. If you accidentally type your password instead of your login name, it may appear in system log files





HUMAN ISSUES



- Even the best password is worthless when someone other knows it.
- Social Engineering.
 - Attacker will extract the password directly from the user.
 - Attacks of this kind are very likely to work unless an organization has a well-thought-out policies.
 - In his 2002 book, The Art of Deception, Mitnick states that he compromised computers solely by using passwords and codes that he gained by social engineering.
 - Motorola case
 - <http://www.youtube.com/watch?v=J4yH2GPiE7o> (3:09)

Kevin Mitnick:

It's much easier to trick someone into giving you his or her password for a system than to spend the effort to hack in.

http://www.youtube.com/watch?v=8_VYWefmy34 (2:00)

Source: Wikipedia. Social engineering



AVOID SOCIAL ENGINEERING & MALICIOUS SOFTWARE

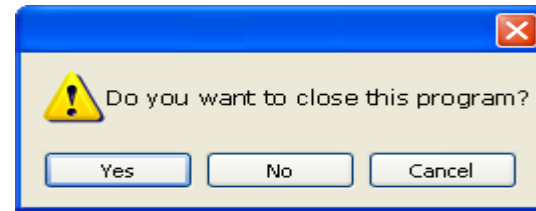
- Do not open email attachments unless you are expecting the email with the attachment and you trust the sender.
- Do not click on links in emails unless you are absolutely sure of their validity.
- Only visit and/or download software from web pages you trust.





OTHER HACKER TRICKS TO AVOID

- Be sure to have a good firewall or pop-up blocker installed
- Pop-up blockers do not always block ALL pop-ups so always close a pop-up window using the 'X' in the upper corner.
- Never click “yes,” “accept” or even “cancel”

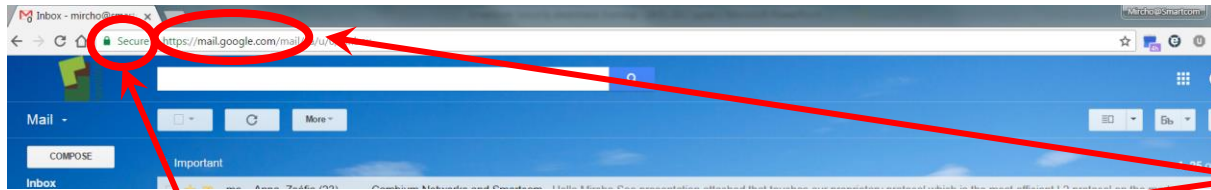


- Infected USB drives are often left unattended by hackers in public places.



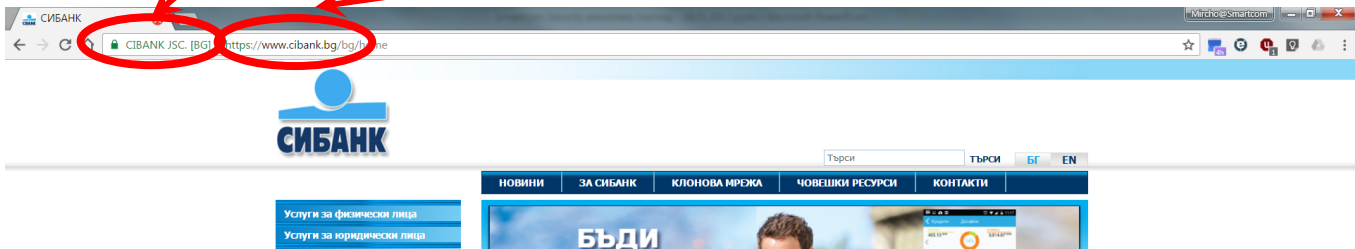
SECURE ONLINE BANKING & BUSINESS

- Always use secure browser to do online activities.
- Frequently delete temp files, cookies, history, saved passwords etc.



Symbol showing enhanced security

https://





Phishing

① Criminally fraudulent process of attempting to acquire sensitive information such as usernames, passwords, credit card details, and other personal information by disguising one's identity in an electronic communication.

- ① Companies
- ① Schools
- ① Airlines
- ① Companies
- ① IT administrators

The image shows a screenshot of a web browser window titled "Advanced card verification". The page features the Visa logo and the text "Advanced verification." Below this, a red warning message reads: "For security reasons please provide information requested below". The form contains the following fields:

- Card Type: A dropdown menu with "Debit" selected.
- Card Number: A single-line text input field.
- Expiration Date: Two separate text input fields separated by a slash (/).
- CVV2: A three-digit text input field.
- ATM PIN: A four-digit text input field.

At the bottom of the form is a "Process" button.



Example phishing/pharming (1/3)



Mail - 2 of 101

COMPOSE

Inbox
Starred
Important
Chats
Sent Mail
Drafts
All Mail
Spam (324)
Bin
Calendar (11)
Downloads
Software

Printer <<printer@smartcom.bg>
to Smartcom

12 Jan (5 days ago)

Please Open the attached document.
This document was sent to you using ES8453 MFP

Resolution: 200 dpi
Color Mode: Auto
Document Size: A4LEF
Sent by: OKI-8453-MFP<ES8453 MFP>
Attachment File Format: Adobe PDF

To view this document, you need to use the Adobe Reader.
To get a free copy of the Adobe Reader, please visit:
<http://www.adobe.com/>

[Untitled].pdf
1.1 MB

Clues

Господа, това проверка от вас ли е?

Good reaction

<http://www.smartcom.bg/link.html>



Example phishing/pharming (2/3)

The screenshot shows a browser window with a 'Dangerous' warning icon in the address bar. The URL is `data:text/html,https://accounts.google.com/ServiceLogin?service=mail`. The page content includes the Google logo, the text 'One account. All of Google.', and a sign-in form with fields for 'Email' and 'Password', and a 'Sign in' button. Below the form are links for 'Stay signed in' and 'Need help?'. At the bottom, there is a 'Create an account' link and a footer with the text 'One Google Account for everything Google' and various service icons.

Symbol showing enhanced security ???

https:// ???



Example phishing/pharming (3/3)

The screenshot shows a phishing page designed to look like a Google login page. At the top is the Google logo. Below it is the text "One account. All of Google." and "Sign in to continue to Google Drive". A grey profile picture placeholder is centered. Below the placeholder are two input fields: the first contains the letter "a", and the second is labeled "Password". A blue "Sign in" button is positioned below the fields. At the bottom left, there is a checked checkbox for "Stay signed in" and a "Need help?" link. At the bottom center, there is a "Create an account" link. At the very bottom, there is the text "One Google Account for everything Google" followed by icons for Google, Gmail, Google Drive, YouTube, Photos, Maps, and Search.

Google Login Phishing Page


The screenshot shows the current authentic Google login page. It features the Google logo at the top, followed by "One account. All of Google." and "Sign in to continue to Gmail". A grey profile picture placeholder is centered. Below the placeholder is a single input field labeled "Enter your email". A blue "Next" button is positioned below the field. At the bottom right, there is a "Need help?" link. At the bottom center, there is a "Create account" link. At the very bottom, there is the text "One Google Account for everything Google" followed by icons for Google, Gmail, Google Drive, YouTube, Photos, Maps, and Search.

Current Authentic Google Login Page



Fake mail (1/2)

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.



Fake mail (2/2)

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 iLowernet Form. This form is required to be completed for all iLowernet users. If you are a former customer of the North Fork bank, using Treasury Optimizer, please use the same button to login and choose Treasury Optimizer form.

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

Click to follow link

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

-0300

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.



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 customers.

Please follow these steps:

1. Open the form at:

http://www.bankofamerica.com/srv_8955/customerse...
<http://www.fgtsssa.co.uk/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.



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.

Or simply get the PayPal update tool 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 information.

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

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

Sincerely,
PayPal

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

To receive email notifications, please go to [Account Settings](#).


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.



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 contact you within 24 hours to discuss the next steps.

Organization Views Extract all files

Name	Type
UPS NR_976120012.exe	Application

Favorite p... N... IIS

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.



Unauthorized remote connection! SLEEPING WARNING

Windows Security Suite

Home Scan History Tools Support



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](#)



BACK-UP IMPORTANT INFORMATION



- No security measure is 100%
- What information is important to you?
- Is your back-up:

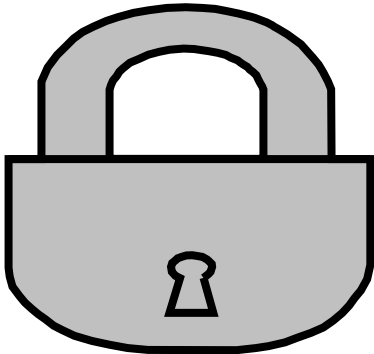
Recent?

Off-site & Secure?

Process Documented?

Tested?

Encrypted?





Securing Yourself

• **Common Sense**

- Awareness/physical security
- Regularly Update Patches
- Anti Virus, anti spyware...
- Be careful what you download
- Read the computer message(s)
- Don't blindly click next > next > next
- Be careful when you read email especially if it belongs to someone else

- Don't try to open every attachment
- Keep your password/PIN to yourself
- Lock your computer while away
- Don't leave SmartCards/Tokens inserted while away
- **Be aware, Be vigilant...**





In Simple Words...

Engage Brain
Before **USING KEYBOARD**





СМАРТКОМ-БЪЛГАРИЯ АД

БИЦ ИЗОТ, офис 317, бул. Цариградско шосе, 7-ми км., 1784 София, България
тел.: +359 2 9650 650, факс: +359 2 9743 469
office@smartcom.bg

Thank you!