The Good Old Days

vintage social networking

LinkedIn  Pinterest  YouTube

foursquare  Instagram  Imgur

WordPress  Twitter  Facebook

reddit  Skype  Tumblr

http://wronghands1.wordpress.com

© John Atkinson, Wrong Hands
What is Cybersecurity

- **Cybersecurity** is the body of technologies, processes and practices designed to protect networks, computers, programs and data from attack, damage or unauthorized access. In a computing context, security includes both **cybersecurity** and **physical security**.
**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.
What’s at risk?

- Theft of money, equipment, and identities
- Reputation
- Loss of customer confidence; loss of business; negatively impacting bottom line
- Service interruption:
  - Internet, email, network resources, etc
Famous Hacks

- Target
- Home Depot
- Stuxnet
- Democratic National Committee
- SWIFT Bank of Bangladesh 81 Mil.

[IRTC Breech Report]
Who’s doing this?

- Phishers
- Spammers
- Bot-Net Operators
- Spyware/Malware Authors
- Hackers
- Activists
- WikiLeaks
- Terrorists
- Foreign Intelligence Services
Threats

Malware: software that is intended to damage or disable computers and computer systems.

Virus: a piece of code that is capable of copying itself and typically has a detrimental effect, such as corrupting the system or destroying data. If it spreads itself through a network it is also known as a Worm.

Spyware: software that enables a user to obtain covert information about another's computer activities by transmitting data covertly from their hard drive.

Adware: software that automatically displays or downloads advertising material (often unwanted) when a user is online.

Crimeware: is designed to perpetrate identity theft through social engineering or technical stealth in order to access a computer user's financial and retail accounts for the purpose of taking funds.

Trojan: is any malicious computer program which is used to hack into a computer by misleading users of its true intent.
Phishing: the fraudulent practice of sending emails purporting to be from reputable companies in order to induce individuals to reveal personal information, such as passwords and credit card numbers.
Phishing and Pretexting

- Attacks are often successive in nature.
- Phone calls and contact may be spaced out by days or weeks to avoid suspicion.
- Used to complete fraudulent wire transfers and gain private information (date of birth, SSN, account information).
- Used to gain access to our systems.
Phishing and Pretexting

Methods of gaining information:

• Ingratiation: “This will impress your supervisor.”
• Conformity: “Everyone else is doing it.”
• Friendship: “Can you help out a friend?”
• Diffusion of Responsibility: “The decision has already been made by your supervisor.”

Other tactics include:

• Rushing you
• Intimidating you
• Name dropping
Phishing and Pretexting

Scammers are sometimes using English as their second language and they give themselves away with poor grammar and bad spelling.

Unsolicited and unexpected email deserve special attention. Emails that threaten dire consequences if you do not respond or comply. Delete without opening and report to IT!

Pop-up messages that claim to be something that it is not.

You may be sent to a website that looks very similar to something legit but is a fake.
Phishing and Pretexting

- Never give out your login credentials to anything!
- Never click on a link or download an attachment in an email that is suspicious.
- Be alert if someone will not give you contact information or is making small mistakes.
- It’s not wrong if you’re suspicious and want to get some verification.
- No system is 100% impenetrable when human interaction is involved. But common sense goes a long way.
- Links can be anywhere and on anything.
Example

From: Helpdesk@thinkfnb.com
Sent: Thursday, February 21, 2015 11:33 AM
Subject: Mailbox Capacity Exceeded

Your mailbox has exceeded its allowable storage space. To improve storage capacity for better functionality of your e-mailbox, you are required to click or copy and paste the below link in a web page, then follow the instruction therein. Click below to enhance mailbox capacity

http://auchibreaking.medianewsonline.com/login.php
Dear Customer,

Your account has been temporarily limited. To remove the limitation from your account please sign in to your online banking to recognize that you are the account holder.

For confirmation, please click the link below:

[Sign In to Bank of America online account](http://teknikismetal.com/kay)

We apologise for any inconvenience caused.
Thank you.

Copyright © 1999-2014 Bank of America Corporation. All rights reserved.
Important Notice
Hey guys Clink on the link below to login to download the Semester Report! Have you received this one?

http://rweas.com/semesterreport/tradefile.php

To keep you inform about the next Semester!

Dear FNB Client,

We have an issue with your FNB Online Banking account.

Click Here to resolve the issue:

http://security-thinkfnb.vea.is-a-soxfan.org/renasant/index.php?activate=R2F98431G

FNB Bank Commercial Banking Security Department.

Message Encrypted

FEXZQVGSMONPISUYSGSLTSTRQWPMNNWWKVLTRKZ
From: Li Xie <xieli@somewhere.edu>
Date: January 15, 2013, 6:03:51 PM CST
To: "info@admin.org" <info@admin.org>
Subject: Message From Administrator

Attention;

An automatic security update has been carried out on your email address. [Click here to complete update](mailto:info@admin.org)

Please note that you have within 24 hours to complete this update. Because you might lose access to your Email Box.

Typos were actually in the message above.
Think before you click......

**Slow Down.** Scammers want you to act first and think later. Never let urgency win out over a careful review.

**Research the facts.** Be suspicious of unsolicited messages. Even if an email comes from a company we do business with, don’t use their link. Use a search engine or a phone directory to contact the company.

**Reject external offers for help.** If you didn’t specifically ask for it from a specific person, refuse the help.
Bank-Hacking Gang Dridex Ramps Up, Branches into Ransomware

By Penny Crosman
March 17, 2016

The top online banking fraud cybergang, Dridex, has recently stepped up its attacks and added ransomware to its repertoire.

Dridex malware already accounts for
**ransomware**

/ˈrænsəmˌweər/  
noun

a type of malicious software designed to block access to a computer system until a sum of money is paid.  
“although ransomware is usually aimed at individuals, it’s only a matter of time before business is targeted as well”

---

**Kentucky hospital hit by ransomware attack**

"Locky" malware holds medical data hostage for a four-bitcoin ransom.

---

Methodist Hospital's information systems director told Krebs that the Locky malware, which came in as an attachment to a spam e-mail, attempted to spread across the network after it had infected the computer it was triggered on. Locky has been known to use malicious scripts in Microsoft Office documents as a means of infecting victims' computers. The malware succeeded in infecting several other systems, prompting the hospital staff to shut down all the hospital's computers. Each PC is brought back online individually after being scanned for telltale signs of Locky while off the network.
Is this spam or a phish? I have not opened it.

Tommy Ellison

Begin forwarded message:

From: Nelly Liew <isabell.chua@gmx.de>
Date: March 22, 2016 at 1:53:21 PM CDT
To: <tellison@cbtx.com>
Subject: Commercial Bank Of Texas Na Payment Due : (001419346)

THIS IS A CONFIDENTIAL COMMUNICATION FOR President, Commercial Bank Of Texas Na. IF YOU ARE NOT THEM, PLEASE DISREGARD AND DELETE IT.

---

Dear Thomas Ellison

Considering that you have not submitted the service termination letter, I am assuming that you may have accidentally missed our invoice 03/1 60035567 (Overdue). Should you decide to cancel the account, please let us know. Note that early withdrawal penalties will apply.

Refer to the enclosed document for billing details.

Regards,

Nelly

---

Nelly Liew | Finance Compliance Department
Kelling Northcross & Nobriga | 1-866-416-5988?
1425 Kxr Piz. Uniondale, New York, 11556

Good Job Mr. E!

Strange Sender

Urgency

Microsoft Office Attachments

Penalties

Don’t Recognize Company and # Doesn’t Work ?
Good Job Rose!

FW: Rose - Unfortunately, Commercial Bank Of Texas Na has an outstanding issue requiring attention

From: Rhonda Burley (mailto:joengerry@juno.com)
Sent: Tuesday, March 15, 2016 1:59 PM
To: Rose REH. Hinton
Subject: Rose - Unfortunately, Commercial Bank Of Texas Na has an outstanding issue requiring attention

This is an important message for Vice President, Commercial Bank Of Texas Na. If you are not them, please ignore and delete it.

Dear Rose Hinton

As we have not received the service cessation letter, I'm presuming that you might have unintentionally overlooked our invoice 02/1600088429 (Past due). If you want to cancel the agreement, please let us know. Note that early withdrawal penalties will apply.

Refer to the enclosed document for billing details.

Kind Regards,
Rhonda

Rhonda Burley | Finance Compliance Department
Amegy Bank National Association | (212) 936-5100
1 Dag Hammarskjold Plz, New York, New York, 10017

Beverly Hills MD
How To Boost Your Skin's Firmness From The Inside Out
http://thirdpartyoffers.juno.com/TGL.3132/56a85b993fc6a58120a08at04duc
Enable macro if the data encoding is incorrect

3XVFC„нІв№ъ…–6уD–©ХЙЇЌKYь?™
ЛсйтР>,Г$\{к‰Б к†д‰У}ЫЇJR7IK9–нN+‘®Шї<ХЇ!Сп$O>–”–
i6[шZSlA‘S•q4тйыяъ’°ЖВСЛzo
IлX3x°0°е”]!ЖДсLгIr □В9й1©фшукoХ†If6yINке€ЪVo–
u•ЙА€ЂIлё©“±IIлщл=о$л‰цy[шглп–
:с©Вч+Ь4ыяДSp[...мфjХшш<имъ<тFbrкуй/”ýдъ>”
Q©л”oРъ”ЯгCg•ka†й6фCBA8MCK>4...k•&тнБ]эLСjXCM”Рлъ*АДцЦвъV
k’...й3нщы§о–<лйн[сs3[□ю5щн?лър}тМ …р
в’Атшш–йФ6Бге>А5’мїёЭ&жf"†5[@йМфтвB†ЖкъИ
<Be©йлВ€·ДжTB…ЖшGгW-
3йк[]й ЁшшO<EBP □@™5 □Hu„,8ИпъуВxм&в□Нег=шЦ™©<v™,йп.ЪQгMг;
•нЕрш[А нЩгГМ±3ъL[йm]рP243––}@шшN4
ою.3K].ГJху.4-»LOЧг“ЖТйCкNРЧЫРГеb
What you may see if you open the bad office document.
Once a victim enables the macros, the macros will download an executable from a remote server and execute it. The file that is downloaded by the macro will be stored in the %Temp% folder and executed. This executable is the Locky ransomware that when started will begin to encrypt the files on your computer and network.

All your files go....POOF!
Ransom Screens

!!! IMPORTANT INFORMATION !!!

All of your files are encrypted with RSA-2048 and AES-128 ciphers.
More information about the RSA and AES can be found here:
http://en.wikipedia.org/wiki/Advanced_Encryption_Standard

Decrypting of your files is only possible with the private key and decrypt program, which is on our secret server.
To receive your private key follow one of the links:

If all of this addresses are not available, follow these steps:
1. Download and install Tor Browser: https://www.torproject.org/download/download-easy.html
2. After a successful installation, run the browser and wait for initialization.
3. Type in the address bar: 6dtxgqam4crv6rr6.onion/F99C410F07678BEF
4. Follow the instructions on the site.

!!! Your personal identification ID: F99C410F07678BEF !!!
Ransom Screens

Attention!

All your main files were encrypted!
ID: ...

Your personal files (documents, databases, jpeg, docx, doc, etc.) were encrypted, their further using impossible.
Encryption was made using a unique public key RSA-2048 generated for this computer.

TO DECRYPT YOUR FILES YOU NEED TO BUY A SOFTWARE WITH YOUR UNIQUE PRIVATE KEY. ONLY OUR SOFTWARE WILL ALLOW YOU DECRYPT YOUR FILES.

NOTE:
- You have only 72 hours from the moment when an encryption was done to buy our software with a loyal price, the payment amount will be increased multiple after the lapse of 72 hours.
- Any attempts to remove this encryption will be unsuccessful. You cannot do this without our software with your key.
- Do not send any emails with threats and rudeness to us. Example of email format: "Hi, I need a decryption of my files. My ID number is ...

(instead of three dots should be your ID number which could be found in the same folder where the encrypted file, also your ID number is shown on this picture)
Contact us by email only, send us an email along with your ID number and wait for further instructions. Our specialist will contact you within 12 hours.
For you to be sure, that we can decrypt your files - you can send us a single encrypted file and we will send you back it in a decrypted form. This will be your guarantee.

Contact information: E-MAIL1: umbredencrypt@engineer.com
E-MAIL2: umbrehelp@consultant.com
Ransom Screens

Cryptolocker

Your Personal files are encrypted!

Your personal files encryption produced on this computer: photos, videos, documents, etc. Encryption was produced using a unique public key RSA-2048 generated for this computer.

To decrypt files you need to obtain the private key.

The single copy of the private key, which will allow to decrypt the files, located on a secret server on the Internet; the server will destroy the key after a time specified in this window. After that, nobody and never will be able to restore files...

To obtain the private key for this computer, which will automatically decrypt files, you need to pay 1.00 bitcoin (~291 USD).

You can easily delete this software, but know that without it, you will never be able to get your original files back.

Disable your antivirus to prevent the removal of this software.

For more information on how to buy and send bitcoins, click “Pay with Bitcoin”
To open a list of encoded files, click “Show files”

Do not delete this list, it will be used for decryption. And do not move your files.

Private key will be destroyed on
1/6/2015 1:11:17 PM

Time left
71:55:27

Checking wallet...
Received: 0.00 BTC

Show files   Pay with Bitcoin
Ransomware Protection

- Online and Air Gapped Frequent Backups
- Bitcoin
- Updated AV
- Malware Bytes Paid Version
- https://www.nomoreransom.org/
Urgency

Looks like Rusty's email but hit Reply and it changes to sergev1020@yahoo.com

Good Job
Brigid!

WIRE / ACH PHISHING
Methods of Physical Access

• Unintentional Access
  – Unlocked doors, public disclosure, **tailgating**.

• Dumpster Diving
  – **Shred anything important**! Don’t keep papers laying around.
Typical Network Home / Office
M&M Security Model
The Human OS

How do we patch these?
### Learning and Self Improvement

#### BLOGS
1. [https://krebsonsecurity.com](https://krebsonsecurity.com)
2. [https://www.troyhunt.com/](https://www.troyhunt.com/)

#### PODCASTS
1. Brakeing Down Security
2. Down the Security Rabbit Hole
3. The Social Engineer Podcast
4. Risky Business
5. Primal Security Podcast
6. Advanced Persistent Threat

#### TV & MOVIES
1. Mr. Robot
2. Black Mirror
3. Viceland’s Cyber War
4. NatGeo’s Breakthrough Cyber Terror
5. Movies: Hackers, WarGames, Snowden

#### YOUTUBE
1. [https://www.youtube.com/watch?v=ku9edEKvGuY](https://www.youtube.com/watch?v=ku9edEKvGuY)
2. [https://www.youtube.com/watch?v=qpvcc9C8SbM](https://www.youtube.com/watch?v=qpvcc9C8SbM)
Social Engineering
Golf Shirt Espionage

JIFFYSHIRTS.com

LANDS’ END
Customize: (For Suggestions or Problems with Customization Process, Please Contact Us)

How do you want to customize your items?

- Change Item Color
- Customize With Artwork
- Customize With Text
Social Engineering Notes

Social Engineering uses influence and persuasion to deceive people by convincing them that the social engineer is someone he is not, or by manipulation.

As a result, the scammer is able to take advantage of people to obtain information with or without the use of technology.
We can follow every best-practice and security recommended by the experts, install every recommended security product, and be thorough and vigilant about properly configuring systems and applying all of our security patches and updates....

We are still completely vulnerable.
Social engineering works so well because

- so many people are by nature helpful
- so many business employees are naturally cheerful and accommodating.

Attacks are rare and most people asking for information or help are legitimate.

- By appealing to our natural tendencies, the attacker will usually be able to use these unscrupulous methods to get what they want.
What You Need To Do

• **BE AWARE!** Awareness is the first and best defense against social engineering and other attacks.
• Understand that there is the potential for attacks and scams. Know the types of ways scammers and social engineers will come at you and how to recognize them.
• Understand the risks and safeguards for preventing attacks and scams.
• Change your mindset: Make it a habit for your mind to check whether something is legit or could be a scam.
• It’s better to be safe than sorry.
Terms You Need to Know

- Router
- Firewall
- Node
- Operating Systems
- IP Address
- Web Browsers
- HTTP vs HTTPS
- Certificates
- Domain Names
- Cookie
- Browser Cache
- Internet of Things
Assess Your Risks

- Identify Your Technology
- Classify Your Data
- Plan Your Mitigations
- Deploy Your Protections
Protection and the 90/10 Rule

- Humans
- Physical Security
- OS + Updates
- Browsers
- Antivirus
- CCleaner
- Malware Bytes
- Express VPN
- Open DNS
- SandBox
- Backups
## Select Operating System

<table>
<thead>
<tr>
<th></th>
<th>Windows</th>
<th>Mac</th>
<th>Linux</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ease of Use</td>
<td>Easy</td>
<td>Easy</td>
<td>Hard</td>
</tr>
<tr>
<td>Security</td>
<td>Bad</td>
<td>Better</td>
<td>Best</td>
</tr>
</tbody>
</table>
Do You Need Whole Disk Encryption?

WINDOWS   BITLOCKER
APPLE FILE VAULT

WARNING: NOT EVERYONE NEEDS THIS!!!
Perform All Updates/Patches

Critical

OS Updates
Browser
Java
Flash
Download Free Versions of Tools

CCleaner – https://www.piriform.com
Malware Bytes - https://www.malwarebytes.com
*Avast - https://www.avast.com

*Don’t trust antivirus 100% no matter the brand
Run CCleaner Daily
Run CCleaner Tools Drive Wiper 1/mo

Very Important
Free Space Only / 1Pass
Run Malware Bytes 1/wk
If you run AV schedule updates and scans daily

Do not rely on AV!!!
www.virustotal.com

Don’t submit files with PII
### Pick a Browser

<table>
<thead>
<tr>
<th>Browser</th>
<th>Compatibility</th>
</tr>
</thead>
<tbody>
<tr>
<td>Chrome</td>
<td><img src="image" alt="Chrome Logo" /></td>
</tr>
<tr>
<td>Safari</td>
<td><img src="image" alt="Safari Logo" /></td>
</tr>
<tr>
<td>Microsoft Edge</td>
<td><img src="image" alt="Microsoft Edge Logo" /></td>
</tr>
<tr>
<td>Microsoft IE</td>
<td><img src="image" alt="Microsoft IE Logo" /></td>
</tr>
<tr>
<td>FireFox</td>
<td><img src="image" alt="FireFox Logo" /></td>
</tr>
</tbody>
</table>

- **It's all about the plugins**
- **Opera and Brave – Meh?**
Install Firefox Plugins
Firefox Plugins

From L to R
Ghostery
AdBlocker Plus
Script Blocker
Blur**
HTTPS Everywhere
Toggle JavaScript
Fortify Firefox

**Privacy**

**Tracking**
- Use Tracking Protection in Private Windows

You can also manage your Do Not Track settings.

**History**
- Firefox will: Never remember history

Firefox will use the same settings as private browsing, and will not remember any history as you browse the Web.

You may also want to clear all current history.

**Location Bar**
- When using the location bar, suggest:
  - History
  - Bookmarks
  - Open tabs

Change preferences for search engine suggestions...
Fortify Firefox with about:config

This might void your warranty!

Changing these advanced settings can be harmful to the stability, security, or performance of this application. You should only continue if you are sure of what you are doing.

- Show this warning next time

I'll be careful, I promise!
Fortify Firefox with about:config

<table>
<thead>
<tr>
<th>Preference Name</th>
<th>Status</th>
<th>Type</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>general.smoothScroll.pixels.durationMaxMS</td>
<td>default</td>
<td>integer</td>
<td>150</td>
</tr>
<tr>
<td>general.smoothScroll.pixels.durationMinMS</td>
<td>default</td>
<td>integer</td>
<td>150</td>
</tr>
<tr>
<td>general.smoothScroll.scrollbars</td>
<td>default</td>
<td>boolean</td>
<td>true</td>
</tr>
<tr>
<td>general.smoothScroll.scrollbars.durationMaxMS</td>
<td>default</td>
<td>integer</td>
<td>150</td>
</tr>
<tr>
<td>general.smoothScroll.scrollbars.durationMinMS</td>
<td>default</td>
<td>integer</td>
<td>150</td>
</tr>
<tr>
<td>general.smoothScroll.stopDecelerationWeighting</td>
<td>default</td>
<td>string</td>
<td>0.4</td>
</tr>
<tr>
<td>general.userAgent.compatibility.mozilla</td>
<td>default</td>
<td>boolean</td>
<td>false</td>
</tr>
<tr>
<td>general.userAgent.locale</td>
<td>default</td>
<td>string</td>
<td>en-US</td>
</tr>
<tr>
<td>general.userAgent.httpsoverride</td>
<td>default</td>
<td>boolean</td>
<td>true</td>
</tr>
<tr>
<td>general.warnings</td>
<td>default</td>
<td>boolean</td>
<td>true</td>
</tr>
<tr>
<td>general.warnOnAboutConfig</td>
<td>default</td>
<td>boolean</td>
<td>true</td>
</tr>
<tr>
<td>geo.enabled</td>
<td>user set</td>
<td>boolean</td>
<td>false</td>
</tr>
<tr>
<td>geo.wifi.xhr.timeout</td>
<td>default</td>
<td>integer</td>
<td>60000</td>
</tr>
<tr>
<td>gestures.enable.single_finger_input</td>
<td>default</td>
<td>boolean</td>
<td>true</td>
</tr>
<tr>
<td>gfx.canvas.azure.backends</td>
<td>default</td>
<td>string</td>
<td>direct2d</td>
</tr>
</tbody>
</table>

Set Value from True to False
Use a VPN on all Wifi

Encrypts and Masks
VPN Tower of Babble
Use Alternative Search Engines
Understand InfoSec Sacrifices

Reduced Usability
Graphically Diminished Experience
Higher Learning Curve
Still Need Strong Passwords
Still Need to Stay Savvy Online
Turn Laptop Completely Off Every Time
Never Stop Learning
Passwords are important

- Make hard passwords
  - Use a phrase, special characters, repeating for complexity
  - Don’t leave in public view
  - Lock your PC when you leave
Multifactor Authentication

- Something You Know
- Something You Have
- Something You Are
TWO FACTOR AUTHENTICATION DEMO
This is why passwords should be changed.

- https://haveibeenpwned.com/
- https://pastebin.com
- https://breachalarm.com/
Identity Theft Tools

- Public Data Websites
- Stolen Checks
- Stolen Wallet IDs, Credit Cards, SS card
- Stolen Mail / “Dumpster Diving” Trash
- Card Skimmers (POS and ATM)
- Genealogy Websites
- Social Media Sites
- Spokeo https://www.spokeo.com/
Garage Sale
Where Do Your Old Computers Go?
Wipe Not Format

https://dban.org/
Wipe Not Format

- Restore all factory settings
- Secure erase all back-ups
- Log out of all social networking sites, applications, emails and company networks
- Use different passwords on multiple systems
Botnets

- Zues or ZBot
  - Acquired thru Spam, Link, Camera, USB
- Installs a Rat (Remote Access Terminal)
- Hides by encryption
- Waits for https call and activates
- Turns on Keylogger and Screen Grabber
- Sends info to anonymous internet account or C&C Server.
Zeus C&C Servers
Corporate Account Takeover

CBTx Online Business Banking

Company ID: 

Company Password: 

User ID: 

User Password: 

Welcome to CBTx Online Business Banking

Terms & Conditions, Privacy, Security