



March 2020





The New Vector

- Things have changed dramatically
- People are not attacking companies directly through networks and hardware that have been secured and have spent millions to secure.
- Don't think about protecting your V.I.P. but think more V.A.P. (Very Attacked People)
- People are the target now instead of direct machine attacks. Why hack their way through networks when they can trick people in giving them access
- Path of Least Resistance is through the people. People embrace convenience before understanding. Baby monitors, Doorbells, teddy bears that can goole can be great things but must be setup correctly





Who are you - The New Vector

- But why do hackers hack at all? Fame, Political, Terrorism, Boredom.
- Physical wars are too expensive and hard to develop without notice
 - 1 Destroyer, couple of planes, small army 10s of Billions
- Average price of Cyber war
 - 10,000 computers, 5,000 credit cards, Specialists \$10k
- They want your CPU, They want your location, they want your social connections, they want to disrupt business, they





Everyone Clicks Eventually

- Everyone clicks on a bad link eventually to save a Nigerian Prince, fix that last minute christmas order, take a quiz, save a dollar and download the next great App.
 - Download an App
 - No App is free. You are always paying for it. Either money or your information
 - Use Airplane mode to play when possible
 - Take a Quiz on social media
 - They want you to lower security
 - They are often just means of tracking



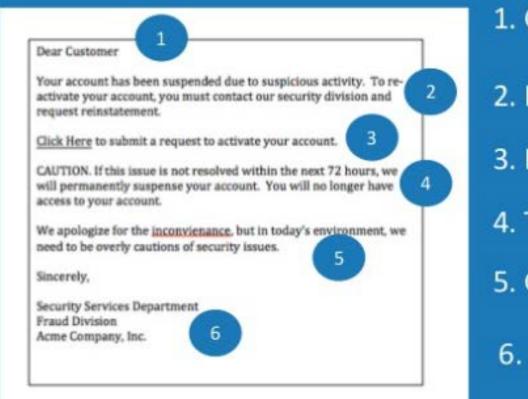


Everyone Clicks Eventually

- On-line Coupons
 - Flood the notifications
 - Personal computers end up running multiple Anti-Virus.
 Then you get the pop ups.
 - Things like adaware and ad removal tools they want you to download are the Virus.
 - Phishing Email Designed to get you to click on a link that you shouldn't
 - Nigerian Prince
 - Fixing a Christmas order
 - Netflix is going to expire



Let's Go Phishing



1. Generic greeting 2. Invokes fear 3. Requires action 4. Threating language 5. Grammar Issues 6. Generic Closing





Let's Go Phishing

Dear Customer

Your account has been suspended due to suspicious activity. To reactivate your account, you must contact our security division and request reinstatement.

http://www.phishingexample.com/48dsfjasdf8 Click H

CAUTION. If this issue is not resolved within the next 72 hours, we will permanently suspense your account. You will no longer have access to your account.

We apologize for the inconvienance, but in today's environment, we need to be overly cautions of security issues.

Sincerely,

Security Services Department Fraud Division Acme Company, Inc. DO hover over links verify its location

DO NOT click on unknown links

DO NOT reply to suspicious requests

DO report the suspected attack





Let's Go Phishing GOOD/BAD site

usbank "		Customer Service Contact Us Locations	
Internet Banki	ng	A A A	
Save time and money with Free Internet Bill Pay!	Welcome to Internet Banking	Enroll in Internet Banking	
Internet Bill Pay lefa you quickly pay all of your bills criane, in one conversiont place. It's completely secure, totally free, and our Risk-Pree Quarantee* means you can be sure every bill is	+ Personal ID + Password	To access your accounts online, enroll now. Need More Info? • What is Internet Banking?	
paid correctly and on time - while you are protected from ble psyments and unauthorized use	Forget your password or need help? Oet login assistance Select Your Destination Your Accounts	 Enequently asked questions. Browser requirements and security standards 	
Once you are logged in to internet Denking, select the Bill Pay link to get started.	Eugin For your security, please remember to log out of internet Banking when you finish your session.	Protect your identity Take a Tour Enroll Now	





Let's Go Phishing GOOD/BAD site

<image/> <image/> <image/> <image/>	Se Edit Yew Pavorkes	jooks Help Addinisi https://wwwf.usbank.com/internetBanking	gRequestRouter/requestCindId=DisplayLogr/Fage	👻 🔁 Ge 🛛 🧣
<page-header><text><section-header><section-header><section-header><section-header><section-header><section-header></section-header></section-header></section-header></section-header></section-header></section-header></text></page-header>		D In Links @ Tis @ Tiatrin W tidey @ Horod	D w Dide C Memberships C UC D UCR-G	CT#
<section-header><section-header><section-header>Control Banking Source Series Source Series</section-header></section-header></section-header>				
Interview In	These		Customer Service Contact Us Locations	
And the provide th	The for here is a second of the			
Save time and mons which Free internet Bain business of your bit order of your bit order of your bit order to the			and the second se	
With Free Internet Bill Pay lets you qaithy reverse Bill reverse Bill <t< td=""><td>Internet Banki</td><td>ng</td><td>ALC -</td><td></td></t<>	Internet Banki	ng	ALC -	
With Free Internet Bill Pay lets you qaithy reverse Bill reverse Bill <t< td=""><td></td><td></td><td></td><td></td></t<>				
With Free Internet Bill Approximate Sile Approximate				
Pay: Login Enrol in Internet Banking Personal ID Personal ID To access your accounts online, enrol ino. Pays do f your bits online, to ony bits online, tony bits ony bits online, tony bits online, to ony bit		Welcome to Internet Banking		
there is the BB Pay let's you quickly and or your bits online, in one or your second to meet the Ip? Out ion assistance. * Personal ID		Legin	Enroll in Internet Banking	
ey el of your bills online, in dee onversiert jakes. Es completoir ter for our bills online - ter our te sure every bills eal controlly and online - the poyments and unauthorized e. More you are logged in to terret Banking, select Year Destination Your Accounts For your security, please remember to log out of Internet Banking when you finish your session Connection Secured Connection Secured	ternet Bil Pey lets you quickly			
House, totally free, and our last the end of the e	ay all of your bills online, in one	P TE SUSSE B		
State free Connection Secured	ecure, totally free, and our	. Designed	And the second	
exit correctly and on the - while you are protected from the payments and unauthorized to: ex. • Select Your Destination: Your Accounts Your Accounts • Connection Secured	and of here of here bold and three streets			
de payments and unauthorized se. • Select Year Destination vis de payments and unauthorized se. • Select Year Destination Your Accounts • Browner requirements and security standards wir wir to get started. • Drive your security, please remember to log out of Internet Banking when you finish your session. • Browner requirements and security standards • Connection Secured • Member FDIC		Forgot your password or need help? Oet login assistance.		
Your Accounts Image: Security Standards Ince you are logged in to terret Banking, select the Ba wy ink to get standed. Image: Security Standards For your security, please remember to log out of Internet Banking when you firesh your session. Image: Security Standards Connection Secured Member FDIC	delikes (one is indeed manufactured destroys).		 ELEMATINY_HARDEN_NAKARENTA 	
Alternation Secured Connection Secured Member 5000		Select Your Destination	 Browser requirements and 	
ery link to get started. For your security, please remember to log out of internet Banking when you finish your session. Connection Secured Member FDIC	te psymentis and unauthorized			
For your security, please remember to log out of Internet Excursi Now Banking when you finish your session Member FDIC	de páyments and unauthorized ree. Ynce you are logged in to		security standards	
Connection Secured Member FDIC	de payments and unauthorized se. Ince you are logged in to ternet Banking, select the B#	Your Accounts 💌	= Protect your identify	
	te payments and unauthorized se. Ince you are logged in to ternet Banking, select the B# ay link to get started.	Your Accounts	Protect your identify Take a Tour	
	te péyments and unauthorized se. Ince you are logged in to ternet Banking, select the B& ay ink to get started.	Your Accounts	Protect your identify Take a Tour	
Weeky Pedge I Security Standards 0 2007 U.S. Barcorp	te péyments and unauthorized se. Ince you are logged in to ternet Banking, select the B& ay ink to get started.	Your Accounts	Protect your identify Take a Tour	
	te payments and unauthorized se. Ince you are logged in to ternet Banking, select the Bill wy ink to get started. Rick Free Guarantee	Your Accounts	Security standards • Protect your identify Take a Tour Enroll Now	





Let's Go Phishing

Log In - Microsoft Internet Esplaner			_191×1
File Edit View Fevorites Tools Help			12
+ task + +	192.00.00		
trigolwin-trip ()www.paypal.com.sd2.us/			• (~60 Links *
This is a subdomain name, NOT part of Paypal.com at all. Depute lots the .ssi2.us - that is the actual website. The paypal.co art of this link comes before the	m	Sign Vp Log. In Help	2
sst2.us - thats a tip off this Welcome Send 1	Maney Request Money M	erchant Tools Auction Tools	_
is a fake websile. Member Log In		Secure Log In 🔒	
Registered users log i	n here. Be sure to protect your (assword.	
PayPal None of these	Sur	tin TLag In THein	
		action Trans	
Contractory and Contractor Contractory			
Member Log In	(Cure Lop 21	
Hadsterad users log in tere, se sura t	o protect your pateword		
Final Address	Porget your preal appleant	Do NOT trust this.	
Passwords	Period your serviced?	Anyone can put a "lock symbol"	
New users sign up herefor or to take	n a renule.	on a website	
This is NOT linked.		Login	
actorit - Account_Lapes / pars / misson / bena data / data / data / count_Cradit	iti, i server i contact is i inar annemer I deferrata i sitoga Utiaga nav	E E Lincontacinez. E	
	n stay company		
Linformation about	to: Payeal All rights received IDIC place through insurance		
	There is	NO LOCK symbol here.	
	This is NO	T a secure page, and is	
	NOT the r	al Pay Pal Login Screen.	
		James C	



Privacy and Security

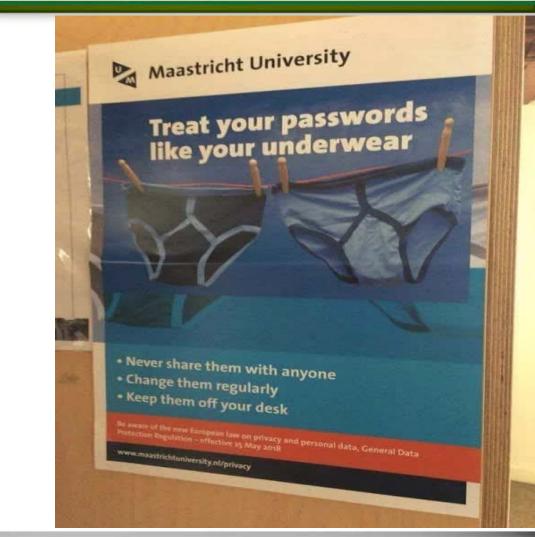
- Are you concerned about Security or are you really concerned about Privacy.
 - My home in 3 months tracked 52 devices coming and going.
 - watches, tablets, some cars, phones, etc
 - A small business can see 100s of devices a day. Keep them of the business network.
- Coffee Shops and Airports and Pineapples
- DO NOT mix work and personal email / data
- Use more than one browser
 - Utilize Privacy or incognito more often





So Many Passwords

- Longer passwords are better
- At a minimum Use different passwords for each subject
 - Credit Cards
 - Bank
 - Shopping
 - Email
 - Streaming
 - Social
 - Work
 - Medical
 - When filling out the security questions used for password recovery do NOT use real information.







Don't Panic - Just change your behavior

- Change your password
- Do not mix work and personal email and data
 - Do not signup for anything with work email. Do not send personal email to work or vice versa. Avoid checking personal info on work networks
- Don't Panic LOOK at the email before clicking. "Hover" over the link to make sure the link is going where you think.
 - Amazon amazon.com; XXX.amazon.com
 - Not amazon amzone.com;amazon.com.XXX; amazon.XXX.com
 - look for HTTPS in the link. When connected look for a lock on the link bar or bottom right of the brower.
- Don't use real information for Security Questions
- Use 2 Factor authentication when possible

cert@sturbridgepd.com 617 429 1598



