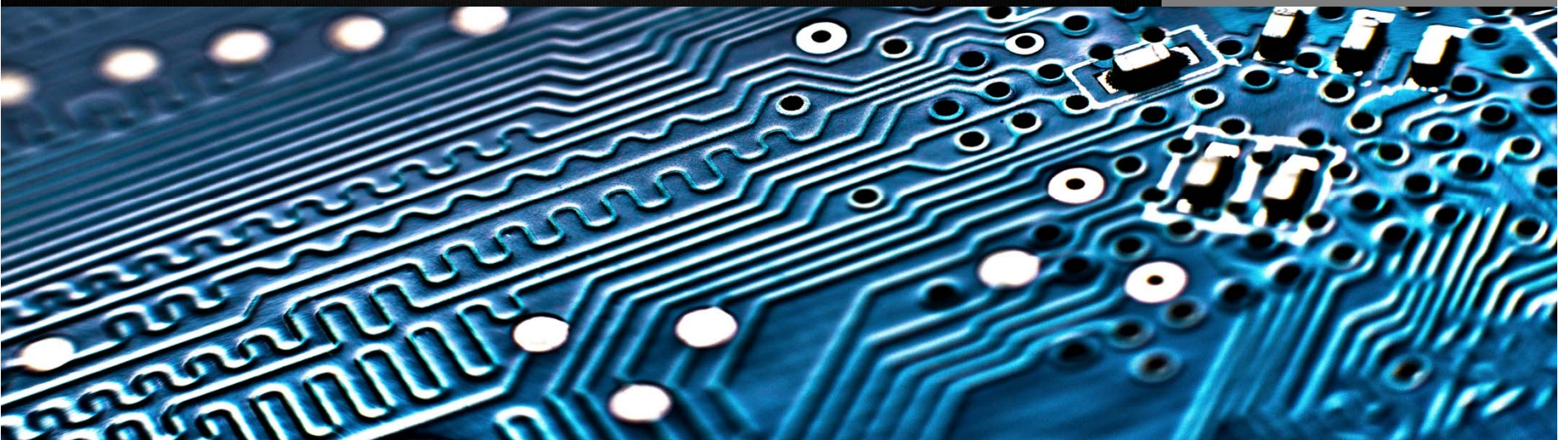


Information Technology Services

Cybersecurity Primer

ACCMA Briefing



Importance of Cybersecurity

- ◎ The internet allows an attacker to work from anywhere on the planet.
- ◎ Risks caused by poor security knowledge and practice:
 - Public Confidence
 - Operations Disruption
 - Identity Theft
 - Monetary Theft
 - Data Theft
 - Legal Ramifications



Some Stats - macro

- The global cost of cybercrime will reach \$6 trillion by 2021
- Greatest transfer of wealth in history
- More profitable than global trade of all illegal drugs combined.



**Source: Cybersecurity Ventures 2018*

Big Picture : CyberSecurity Encompasses hundreds of elements at different levels



Easy to get lost in the noise.....

Reality

- Changing tech behavior – culture item
- Focus on what will really mitigate risks
- Education of employees is core ←
- Additional layers don't mitigate all risk
- 3 primary risks that emerge



3 Major Risk Points

- Passwords: The most critical aspect of password security is *how* people use their passwords.
- Phishing: The focus here is on identifying indicators of phishing emails.
- Backups: Now more important than ever...but are they current & tested?



1) Password Dilemma

- 98% of employees do not have an *effective* strategy on passwords
- **60% of employees use the exact same password for everything they access**
- NEVER SHARE IT WITH ANYONE!
- Be at least ten characters with special characters



Pa s s w o r d s

number of Characters	Numbers only	Upper or lower case letters	upper or lower case letters mixed	numbers, upper and lower case letters	numbers, upper and lower case letters, symbols
3	Instantly	Instantly	Instantly	Instantly	Instantly
4	Instantly	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	Instantly	3 secs	10 secs
6	Instantly	Instantly	8 secs	3 mins	13 mins
7	Instantly	Instantly	5 mins	3 hours	17 hours
8	Instantly	13 mins	3 hours	10 days	57 days
9	4 secs	6 hours	4 days	1 year	12 years
10	40 secs	6 days	169 days	106 years	928 years
11	6 mins	169 days	16 years	6k years	71k years
12	1 hour	12 years	600 years	108k years	5m years
13	11 hours	314 years	21k years	25m years	423m years
14	4 days	8k years	778k years	1bn years	5bn years
15	46 days	212k years	28m years	97bn years	2tn years
16	1 year	512m years	1bn years	6tn years	193tn years
17	12 years	143m years	36bn years	374tn years	14qd years
18	126 years	3bn years	1tn years	23qd years	1qt years

In 2010, an 8 character password made up of both upper and lower case letters, numbers and symbols would have taken 2.25 years to crack. The same password now would take just 57 days.



Key:

k – Thousand (1,000 or 10³)

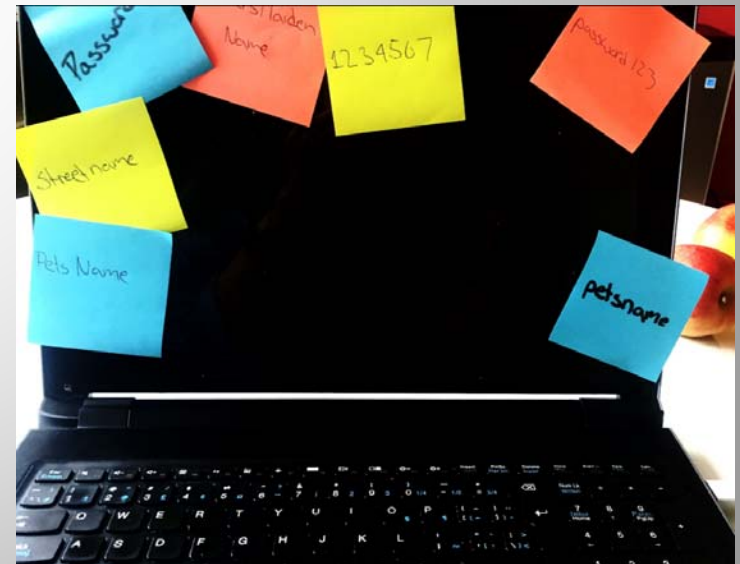
m – Million (1,000,000 or 10⁶)

bn – Billion (1,000,000,000 or 10⁹)

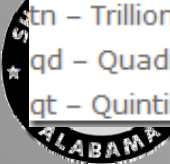
tn – Trillion (1,000,000,000,000 or 10¹²)

qd – Quadrillion (1,000,000,000,000,000 or 10¹⁵)

qt – Quintillion (1,000,000,000,000,000,000 or 10¹⁸)



*Source: Author Mike Halsey "Troubleshooting Windows 1st Edition"

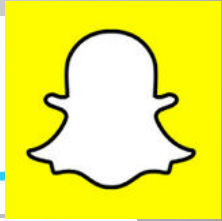


Dark Web – Selling for less than \$0.01 per email address & password: TOR, Freenet, I2P, Onionland

60% of employees use the exact same password for everything they access

The screenshot displays a marketplace interface with four product listings. Each listing includes a logo (Yahoo! or Gmail), a title, price, vendor information, and a 'Buy Now' button.

Product	Price (USD)	Quantity	Vendor	Class	Delivery
Yahoo 100K Email:Pass Decrypted Instant Delivery	USD 10.75	1	SunTou683	Digital	Instant Delivery
Yahoo 145K Email:Pass Decrypted Instant Delivery	USD 13.76	1	SunTou683	Digital	Instant Delivery
Gmail 50K Email:Pass Decrypted Instant Delivery	USD 28.24	1	SunTou683	Digital	Instant Delivery
Gmail 450K Email:Pass Decrypted Instant Delivery	USD 25.74	1	SunTou683	Digital	Instant Delivery



Creating Strong Passwords

- **Develop a strategy.** Numbers only going to escalate
- **Use a phrase.**
- ABT2_uz_AMZ! (About to use Amazon)
- Pwr4Acct-\$\$ (Password for account at bank)
- Pwr4Acct-Fb (Password for account at Facebook)
- 4Score&7yrsAgo (Four score and seven years ago - from the Gettysburg Address)
- John3:16=4G (Scriptural reference)
- Go Sea 5helby! (easy to remember, spaces make it very secure)



LastPass...



2) Phishing

- Email method of fraudulently acquiring sensitive information via trickery.
- Your employees are the primary targets, they ought to be prepared, informed, weaponized as your first line of defense.
- Training employees how to recognize and react to phishing emails is your best security ROI.



Real Metrics – Email

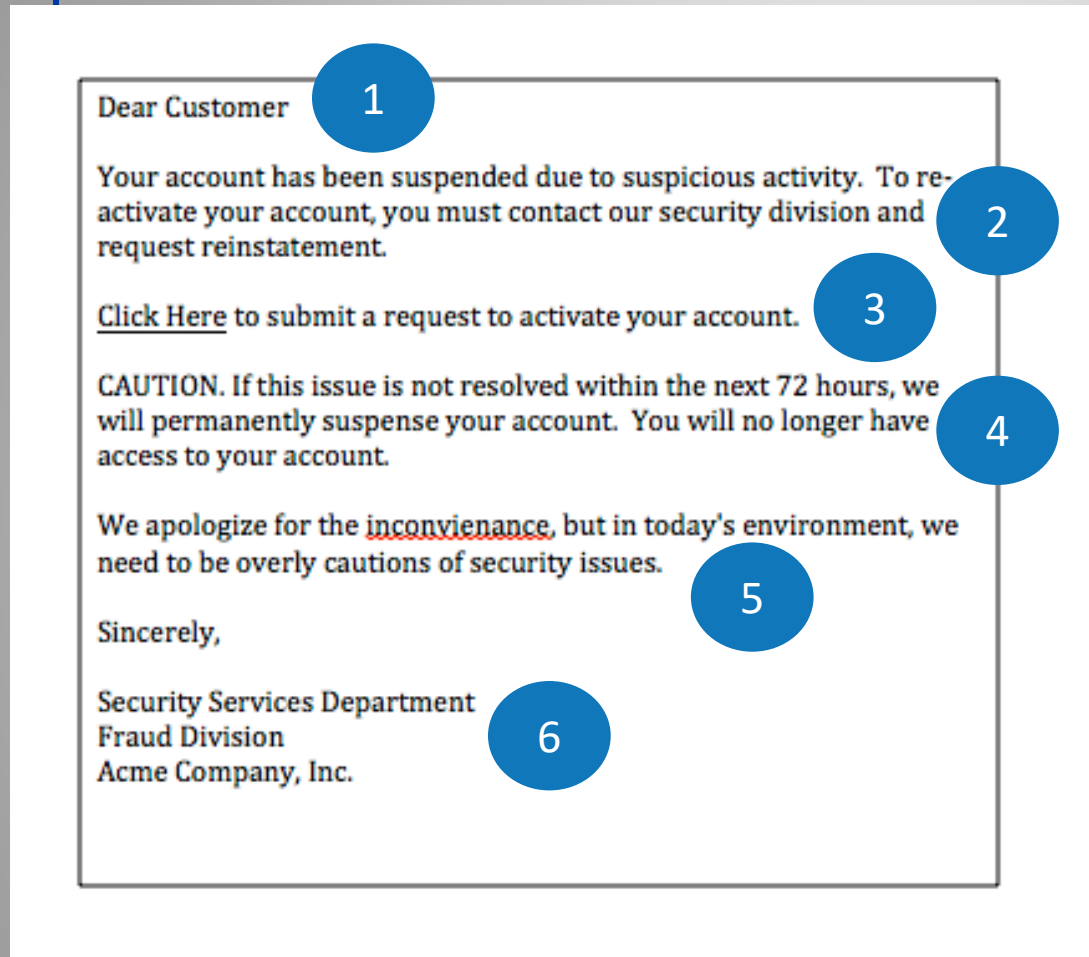
Email Statistics [inbound]				Help
	TOTAL	DAY	HOUR	
Blocked	28,885,249	2,533	480	
Blocked: Virus	320,348	80	11	
Rate Controlled	3,298,417	423	166	
Quarantined	166,581	23	3	
Allowed: Tagged	496,310	58	11	
Allowed	3,234,358	227	40	
Total Received	36,401,263	3,344	711	

92% Blocked

8% Allowed



Common Phishing Traits



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



Hyp e rlink Risks

Dear Employee,

According to our AUP, you will have to confirm your e-mail by the following link, or your account will be suspended for security reasons.

<http://www.shelbyal.com/safeConfirm>

After following the instructions in the sheet, your account will not be interrupted and will continue as normal.

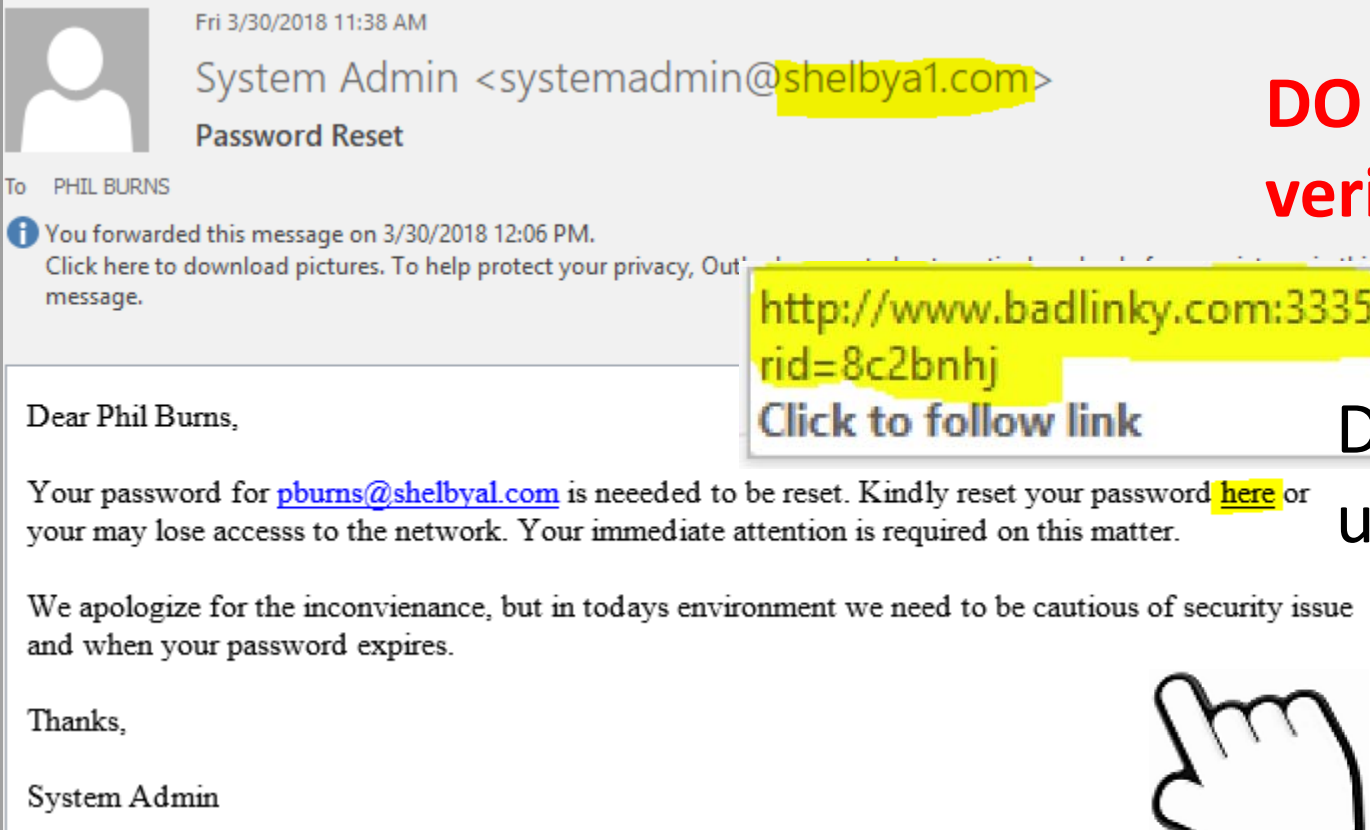
Thanks for your attention to http://www.nbmd.cn/Confirmation_Sheet.pif any inconvenience.

Sincerely,

Phil



What To Do



**DO hover over links
verify location**

**DO NOT click on
unknown links**



**DO NOT reply to
suspicious requests**

16%

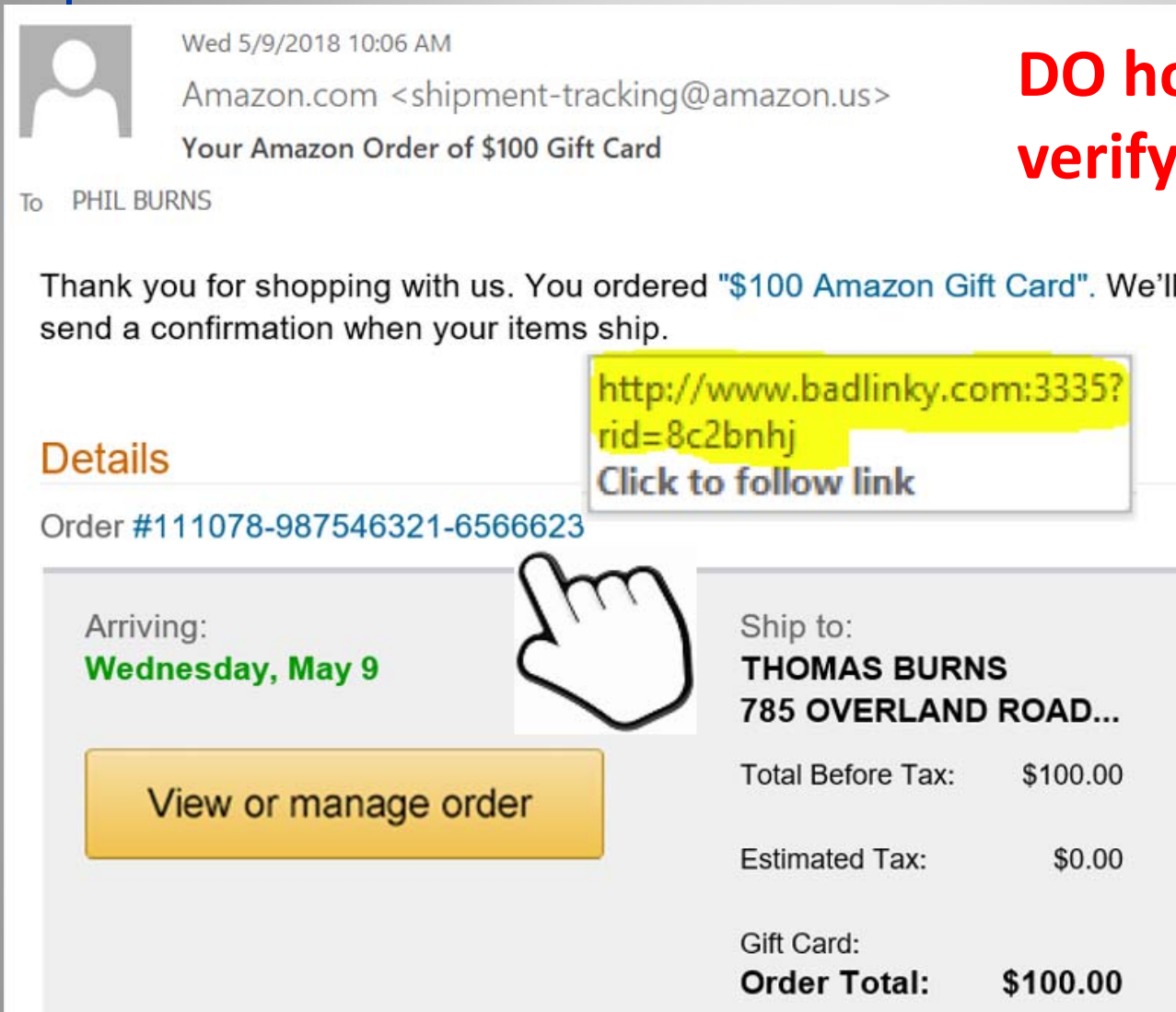


What To Do

**DO hover over links
verify its location**

DO NOT click on
unknown links

DO NOT reply to
suspicious requests



Wed 5/9/2018 10:06 AM
Amazon.com <shipment-tracking@amazon.us>
Your Amazon Order of \$100 Gift Card

To PHIL BURNS

Thank you for shopping with us. You ordered "[\\$100 Amazon Gift Card](#)". We'll send a confirmation when your items ship.

[http://www.badlinky.com:3335?rid=8c2bnhj](#)
Click to follow link

Details

Order #111078-987546321-6566623

Arriving:
Wednesday, May 9

[View or manage order](#)

Ship to:
THOMAS BURNS
785 OVERLAND ROAD...

Total Before Tax:	\$100.00
Estimated Tax:	\$0.00
Gift Card:	
Order Total:	\$100.00

5%





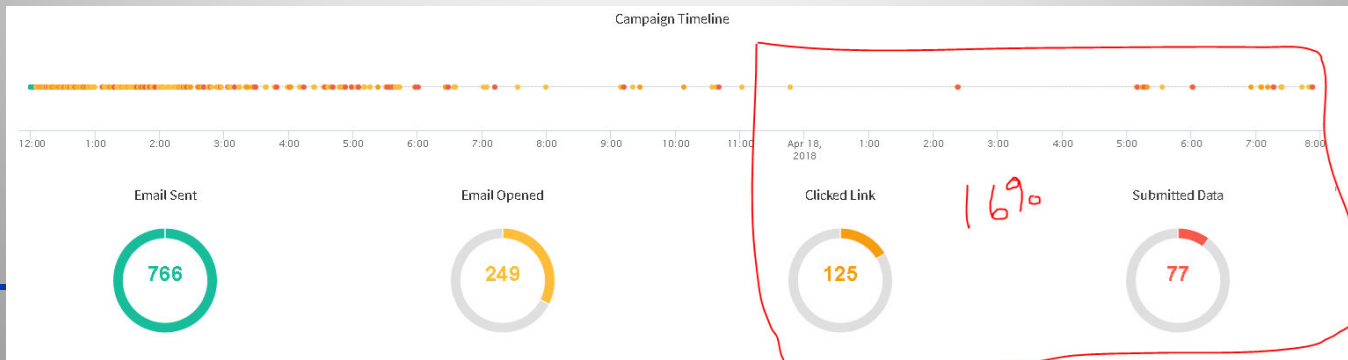
If they clicked...

BUSTED

For those that submitted information and were redirected to this page, you will be sent information for a **mandatory** 1 hour class on CyberSecurity. Meanwhile, please review the information below.

We created this **fictitious** phishing operation as part of our CyberSecurity education series to ensure Shelby County employees and our partners are well trained to recognize and understand the current threats that may arrive in your email. This is the same technique that was used to lock down servers on thousands of public and private companies.

Education is the key to first recognize then stop a phishing attempt. Let's review each of the FOUR elements below that should have prevented you from arriving at this destination.



Is ur home or work email account listed? If so, change psw for that service (adobe, coupon sites, Linked in, etc.)

The screenshot shows a web browser window with the URL <https://haveibeenpwned.com>. The browser's address bar and tabs are visible at the top. The website's navigation menu includes links for Home, Notify me, Domain search, Who's been pwned, Passwords, API, About, and Donate. The main content area features a large white rounded rectangle containing the text `';--have i been pwned?`. Below this is the instruction "Check if you have an account that has been compromised in a data breach". A search input field contains the email address `cio@shelbyal.com`, and a dark button labeled "pwned?" is positioned to its right. The result section displays "Good news — no pwnage found!" followed by "No breached accounts and no pastes (subscribe to search sensitive breaches)". At the bottom, there are links for "Notify me when I get pwned" and "Donate", along with social media icons for Facebook and Twitter.



Sun 6/3/2018 1:47 AM

Have I Been Pwned <noreply@haveibeenpwned.com>

2 emails on shelbyso.com have been pwned in the Ticketfly data breach

To PHIL BURNS

You signed up for notifications when emails on **shelbyso.com** were pwned in a data breach and unfortunately, it's happened. Here's what

Breach:	Ticketfly
Date of breach:	31 May 2018
Accounts found:	26,151,608
Your accounts:	2
Compromised data:	Email addresses, Names, Phone numbers, Physical addresses
Description:	In May 2018, the website for the ticket distribution service Ticketfly was defaced by an attacker and was subsequently taken offline . The attacker allegedly requested a ransom to share details of the vulnerability with Ticketfly but did not receive a response. Ticketfly is a well-known and trusted brand in the ticket industry and the breach could have had significant consequences for its users.



From: PHIL BURNS
Sent: Thursday, November 16, 2017 6:15 PM
To: [REDACTED]>
Subject: CyberSecurity Alert

We have started a new proactive program to monitor all ShelbyAl.com & ShelbySO.com email addresses that appear on “Dark Web” (click wiki definition) web sites. Your specific address was recently found associated with a breached password for the services noted below. This DOES NOT mean your County network password or email has been breached in anyway....however it could mean your account with these online services below have so if you are actively using these services the best next step would be to reset your password with this service. Please make sure you do not use your County network password on any online accounts as this does expose our network to some risk. Please let me know if you have any questions.

Email	Breach
[REDACTED]	PoliceOne

Phil Burns
Chief Operating Officer
IT, Personnel Services, Community Services, License Operations
Shelby County, Alabama
102 Depot Street
Columbiana, Alabama 35051
(205) 670-6999 (Office)
(206) 670-6993 (Fax)
pburns@shelbyal.com

From: Have I been pwned? [<mailto:noreply@haveibeenpwned.com>]
Sent: Thursday, November 16, 2017 6:07 PM
To: PHIL BURNS <PBURNS@shelbyal.com>
Subject: email on shelbyal.com have been pwned in the Coupon Mom / Armor Games data breach (unverified)



An email on a domain you're monitoring has been pwned



Real-time updates on Alerts...into security layers



16 NOV 2017

Alert Number

AC-LD000088-MW

WE NEED YOUR HELP!

If you find any of these indicators on your networks, or have related information, please contact **FBI CYWATCH** immediately.

Email:



The following information is being provided by the FBI, with no guarantees or warranties, for potential use at the sole discretion of recipients in order to protect against cyber threats. This data is provided to help cyber security professionals and system administrators guard against the persistent malicious actions of cyber criminals.

This FLASH has been released **TLP:AMBER**. Recipients may only share **TLP:AMBER** information with members of their own organization, and with clients or customers who need to know the information to protect themselves or prevent further harm.

Additionally, the dissemination of this FLASH is limited to entities engaged in Energy Critical Infrastructure only, and not approved for dissemination outside of the Energy Critical Infrastructure.

Targeting of US Energy Companies

Summary

Cyber actors targeted companies in the US energy sector from August to September 2017 using spear phishing emails with malicious attachments,

- 173.208.222.34
- 59.90.93.97
- 91.213.31.30
- 111.207.78.204
- 181.119.19.56
- 184.107.209.2
- 80.91.118.45
- 211.233.13.62
- 211.236.42.52
- 211.49.171.243
- 221.138.17.152
- 108.222.149.173
- 176.35.250.93
- 41.131.29.!
- 64.86.34.2.
- 98.101.211
- 98.101.211
- 108.222.14

DOMAIN:

- www.unsu

FILENAME:

- C:\Svchost.
- C:\%CURRE
- Csc.exe
- Leo.exe
- Proquota
- 비트코인_
- Job Descrip

URLs:

- https://deltaemis.com/CRCForm/3E_Com%20Description.doc (likely compromised)
- <http://link.gmgb4.net/x/c?c=1318538&l=9111-f101200d033e&r=3c616eaa-117f-40> (likely compromised website)
- <http://104.192.193.149/Event/careers/job7.doc>
- <http://210.202.40.35/CKRQST/Company/>

YARA SIG:

```
rule Shock_and_Yawn
{
```

Examples



General rule: Avoid hyperlink in email on external...go direct to site in browser

FILE MESSAGE

Ignore Delete Reply Forward Meeting Move to: ? Rules Mark Unread Translate Zoom

Delete Respond Quick Steps Move Actions Tags Editing Zoom

Thu 6/29/2017 1:43 PM
infragardteam@ignconnect.org
Private Industry Notification - Individuals Threatening Distributed Denial of Service of Private-Sector Companies for Bitcoin

To PHIL BURNS

Attention InfraGard member,

You have received a new broadcast message.

A Private Industry Notification (PIN) titled "Individuals Threatening Distributed Denial of Service of Private-Sector Companies for Bitcoin" has been posted to the InfraGard system.

Summary
An individual or group claiming to be "Anonymous" or "Lizard Squad" sent extortion emails to private-sector companies threatening to conduct distributed denial of service (DDoS) attacks on their network unless they received an identified amount of Bitcoin. No victims to date have reported DDoS activity as a penalty for non-payment.

Threat
In April and May 2017, at least six companies received emails claiming to be from "Anonymous" and "Lizard Squad" threatening their companies with DDoS attacks within 24 hours unless the company sent an identified amount of Bitcoin to the email sender. The email stated the demanded amount of Bitcoin would increase each day the amount went unpaid. No victims to date have reported DDoS activity as a penalty for non-payment.

To read this document you must login to the InfraGard system. This document is located on the secure site: Publications > Documents > Flash & Pins.

Please contact InfraGard Tech Support at 877.861.6298 for account assistance, including a password reset or user name recovery.

Please log in to ~~<https://www.infragard.org>~~ to view the message.

https://www.infragard.org

USE YOUR INFRAGARD ACCOUNT

User Name
Password
Reset Password

InfraGard
Partnership for Protection

Cyber Forensics Camp
July 21, 2017 | Dynetics, 1002 Explorer Blvd. Huntsville, AL
Registration from May 10th through June 30th

LEARN MORE

HOME FBI NEWS FEED CHAPTERS EVENTS

WELCOME TO INFRAGARD





Log In

Having trouble logging in?

The "S"

Good Site or Bad?

The screenshot shows a web browser window with the address bar displaying `http://www.regions.com.bank4u.com/personal-banking`. The page features the Regions Bank logo and navigation menus for "Locations", "Services", "Open an Account", "Careers", "Contact Us", and "En Español". Below the logo, there are tabs for "Personal", "Small Business", "Commercial", "Wealth", and "Insights", with "Personal" selected. A search bar is also present. The main content area is a green banner for "Online Banking Login", which includes fields for "Online ID" and "Password", a "Log In" button, a "Remember Me" checkbox, and a link for "Forgot Online ID or Password?".



Good Site or Bad?

The screenshot shows a web browser window with a single tab titled "Banking Services: Checkin...". The address bar displays "https://www.regions.com/personal-banking". The website header features the "REGIONS" logo and navigation links for "Personal", "Small Business", "Commercial", "Wealth", and "Insights". Below this is a secondary navigation bar with "Bank", "Save & Invest", "Borrow", and "Insure". The main content area is a green banner for "Online Banking Login", which includes links for "Enroll in Online Banking" and "Privacy & Security". The login form contains two input fields: "Online ID" and "Password", a "Remember Me" checkbox, and a "Forgot Online ID or Password?" link.





- You will confirm to the sender that your email address is both valid and in active use.
- By responding to the email, you will positively confirm that you have opened and read it.
- If your response goes back via email, they will have your email client & IP
- The most scary of all, the link may download malware on your PC or worse.



Petya

Oops, your important files are encrypted.

If you see this text, then your files are no longer accessible, because they have been encrypted. Perhaps you are busy looking for a way to recover your files, but don't waste your time. Nobody can recover your files without our decryption service.

We guarantee that you can recover all your files safely and easily. All you need to do is submit the payment and purchase the decryption key.

Please follow the instructions:

1. Send \$300 worth of Bitcoin to following address:

1Mz7153HMuxXTuR2R1t78mGSdzaAtNbBWX

2. Send your Bitcoin wallet ID and personal installation key to e-mail wowsmith123456@posteo.net. Your personal installation key:

74f296-2Nx1Gm-yHQRWr-S8gaN6-8Bs1td-U2DKui-ZZpKJE-kE6sSN-o8tizU-gUeUMa

If you already purchased your key, please enter it below.
Key: _

Wanna Decrypt

Wanna Decrypt0r 2.0

Oops, your files have been encrypted!

What Happened to My Computer?
Your important files are encrypted. Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

Can I Recover My Files?
Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time. You can decrypt some of your files for free. Try now by clicking <Decrypt>. But if you want to decrypt all your files, you need to pay. You only have 3 days to submit the payment. After that the price will be doubled. Also, if you don't pay in 7 days, you won't be able to recover your files forever. We will have free events for users who are so poor that they couldn't pay in 6 months.

How Do I Pay?
Payment is accepted in Bitcoin only. For more information, click <About bitcoin>. Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>. And send the correct amount to the address specified in this window. After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am

Payment will be raised on 5/15/2017 15:58:08
Time Left 02:23:58:59

Your files will be lost on 5/19/2017 15:58:08
Time Left 06:23:58:59

Send \$300 worth of bitcoin to this address:
115p7UMMngoJ1pMvKpHjicRdfJNXj6LrLn

Check Payment Decrypt

To o La te ..

Ra nso m wa re

Noob

YOUR IMPORTANT DATA HAS BEEN ENCRYPTED

Your Documents, Photos, Videos, and other important files has been encrypted.

The only way to restore your data is you must pay 3 BTC to my wallet address. To complete your payment please contact me at: geekhaxid[at]gmail.com, and get your private key to decrypt your files

Your data will be safe until 24 hours. If in 24 hours I'm not receive the payment your data will be encrypted forever.

Big Thanks,
noob

Cryptolocker

Your personal files are encrypted!

Your important files encryption produced on this computer: photos, videos, documents, etc. [Here](#) is a complete list of encrypted files, and you can personally verify this.

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 you 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 **300 USD / 300 EUR** / similar amount in another currency.

Click «Next» to select the method of payment and the currency.

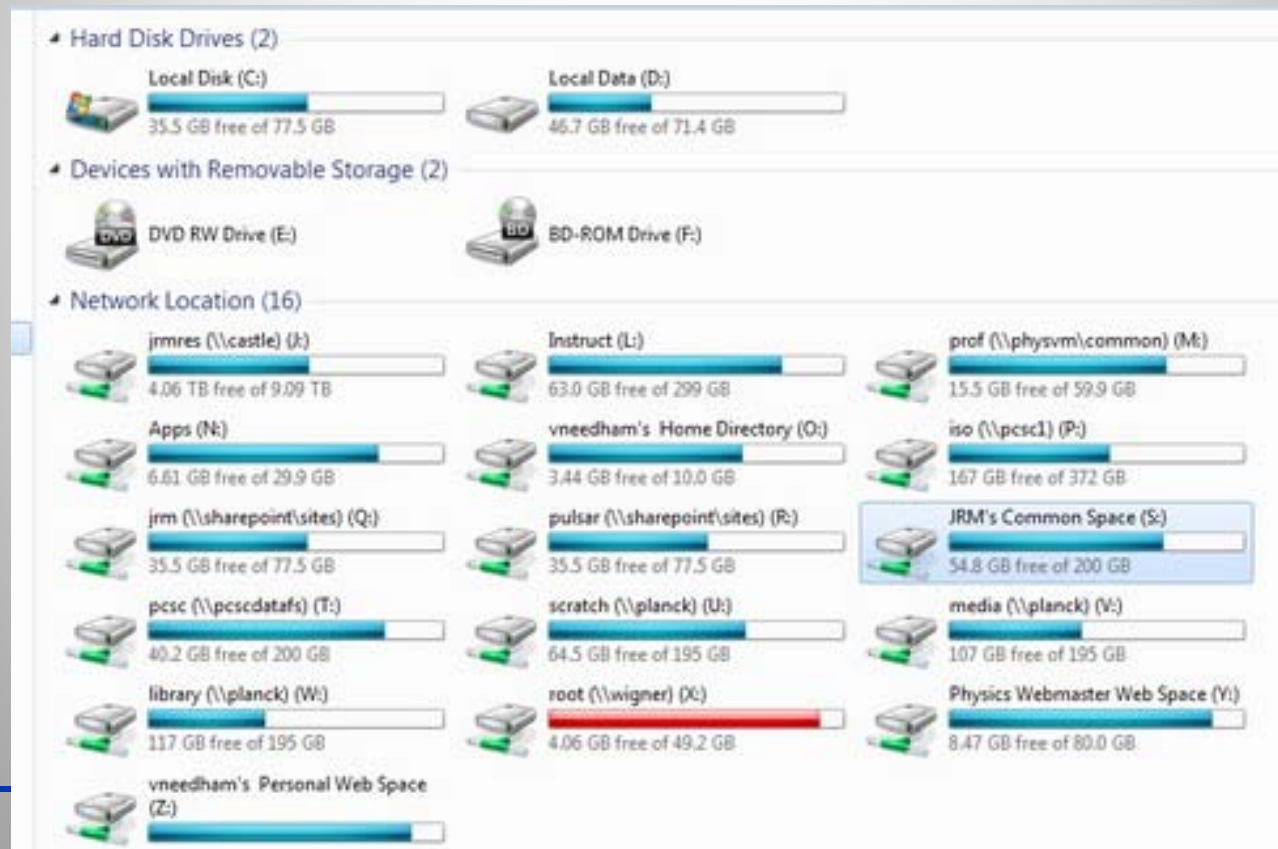
Any attempt to remove or damage this software will lead to the immediate destruction of the private key by server.

Private key will be destroyed on 9/15/2013 8:44 PM

Time left 57:45:37

Next >>

Ransomware is a type of malware that locks your files, data or the PC itself and extorts money from you in order to provide access.



3) Backups

- ◎ Backups has never been more important!
- ◎ No security measure is 100% reliable.
- ◎ Even the best hardware fails.
- ◎ What information is important to you?
- ◎ Is your backup:



- Recent?
- Off-site & Secure?
- Encrypted?
- Tested?

VEEAM

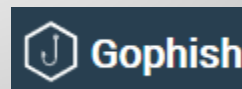


8 Take Aways

- Only use business email for business. Many nefarious groups tap shopping sites email data.
- Only use business web browsing for business. Many shopping sites have a poor track record for controlling plugins and other code running on their sites.
- Do not use online email at work (while on a networked device). Many security layers are bypassed by opening external mail on network.
- Use **extreme** caution when clicking any hyperlink within an email.
- Stay on latest version of operating system and maintain all key security patches (to the extent possible w/ applications).
- Encrypt mission critical data stores on PC's, Servers and ALL portable data which includes iphones, USB thumb drives, tablets, laptops, etc.
- Ensure core PC's are backed up on a regular schedule (with ransomware, restore from backup is only remedy)
- Ensure virus/malware control are up to date and active on all PC's that are used – home & work – any data at rest (thumbs, cloud storage, etc.)



Setup Bank/CC Account Notifications



<https://haveibeenpwned.com/>

End

- CyberSecurity is a culture...

Phil Burns

Shelby County, Alabama

(205) 670-6999 (Office)

pburns@shelbyal.com

