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.

8 to 10 digits
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.

*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
Creating Strong Passwords

- **Develop a strategy.** Numbers only going to escalate
- **Use a phrase.**
- ABT2_uz_AMZ! (About to use Amazon)
- Pwrd4Acct-$$(Password for account at bank)
- Pwrd4Acct-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)
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

92% Blocked
8% Allowed
Common Phishing Traits

1. Generic greeting
2. Invokes fear
3. Requires action
4. Threating language
5. Grammar Issues
6. Generic Closing
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 this request. We apologize for 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

Dear Phil Burns,

Your password for pburns@sabylba1.com is needed to be reset. Kindly reset your password here or your may lose access to the network. Your immediate attention is required on this matter.

We apologize for the inconvenience, but in today's environment we need to be cautious of security issues and when your password expires.

Thanks,

System Admin
What To Do

DO hover over links verify its location

DO NOT click on unknown links

DO NOT reply to suspicious requests

5%

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

Order #111078-987546321-65666623

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

<table>
<thead>
<tr>
<th>Breach:</th>
<th>Ticketfly</th>
</tr>
</thead>
<tbody>
<tr>
<td>Date of breach:</td>
<td>31 May 2018</td>
</tr>
<tr>
<td>Accounts found:</td>
<td>26,151,608</td>
</tr>
<tr>
<td>Your accounts:</td>
<td>2</td>
</tr>
<tr>
<td>Compromised data:</td>
<td>Email addresses, Names, Phone numbers, Physical addresses</td>
</tr>
<tr>
<td>Description:</td>
<td>In May 2018, the website for the ticket distribution service <a href="https://www.thehackernews.com/2018/05/ticketfly-tickets-breach.html">Ticketfly was defaced by an attacker and was subsequently restored</a> after the attacker allegedly requested a ransom to share details of the vulnerability with Ticketfly but did not receive a response. The attack was reported to authorities and the affected data includes subscribers' emails.</td>
</tr>
</tbody>
</table>


From: PHIL BURNS
Sent: Thursday, November 16, 2017 6:15 PM
To: CyberSecurity Alert
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.

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)
(205) 670-6993 (Fax)
pburns@shelbyal.com

From: Have I been pwned? [mailto:noreply@havebeenpwned.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
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.
Examples
General rule: Avoid hyperlink in email on external ....go direct to site in browser

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.
The "S"
Good Site or Bad?
Good Site or Bad?
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.

Email: To unsubscribe or not?? .............NOT.
Too Late.. Ransomware

Petya

Cryptolocker

Wanna Decrypt
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?
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.)
End

• CyberSecurity is a culture...

Phil Burns
Shelby County, Alabama
(205) 670-6999 (Office)
pburns@shelbyal.com