



Guiding Philanthropy through Technology

# How to Build Your Own Escape Room





## **Bob Hewitt - CIO**

- CISSP, GSEC, GCIH, GPEN, GWAPT, CIPP/e
- SANS Community Instructor
- [linkedin.com/in/bobhewitt/](https://www.linkedin.com/in/bobhewitt/)
- @infosecbobh



## **Justin Perkins**

- Systems Administrator
- Game Master
- Lego Builder

# Death by PowerPoint



- Annual and new hire
- 50+ Slides
- > 2hours

# Escape Room



- 60 Minute Real Life Adventure Game
- Themed room
- Find hidden clues
- Solve challenging puzzles
- Requires Teamwork, Speed, Creativity, and Patience



# Where to Start?

- Define your objectives
- Make it relatable to all groups
- Build teams that builds teams

# The Mission



You have been assigned to the Information Security Team. (Yes! Your dream job!) Sadly an adversary has compromised one credit card record, that's right, one!

A separate team is looking into how this happened, while your job is to define the scope of the breach to the single record, otherwise we may have an obligation to report to every credit card user on the system.



# Rules

- The game master is always right.
- 60 Minute limit.
- All information associated with the game is classified as confidential and will be downgraded once all teams have completed.
- All policies and procedures must be followed.
- Workstations and partitions cannot be moved.
- The game master is always right....Really!





# Penalties

- Hints upon request: 5 Minutes
- Security policy fail: 5 Minutes
- Breaking of a General Rule: 5 Minutes

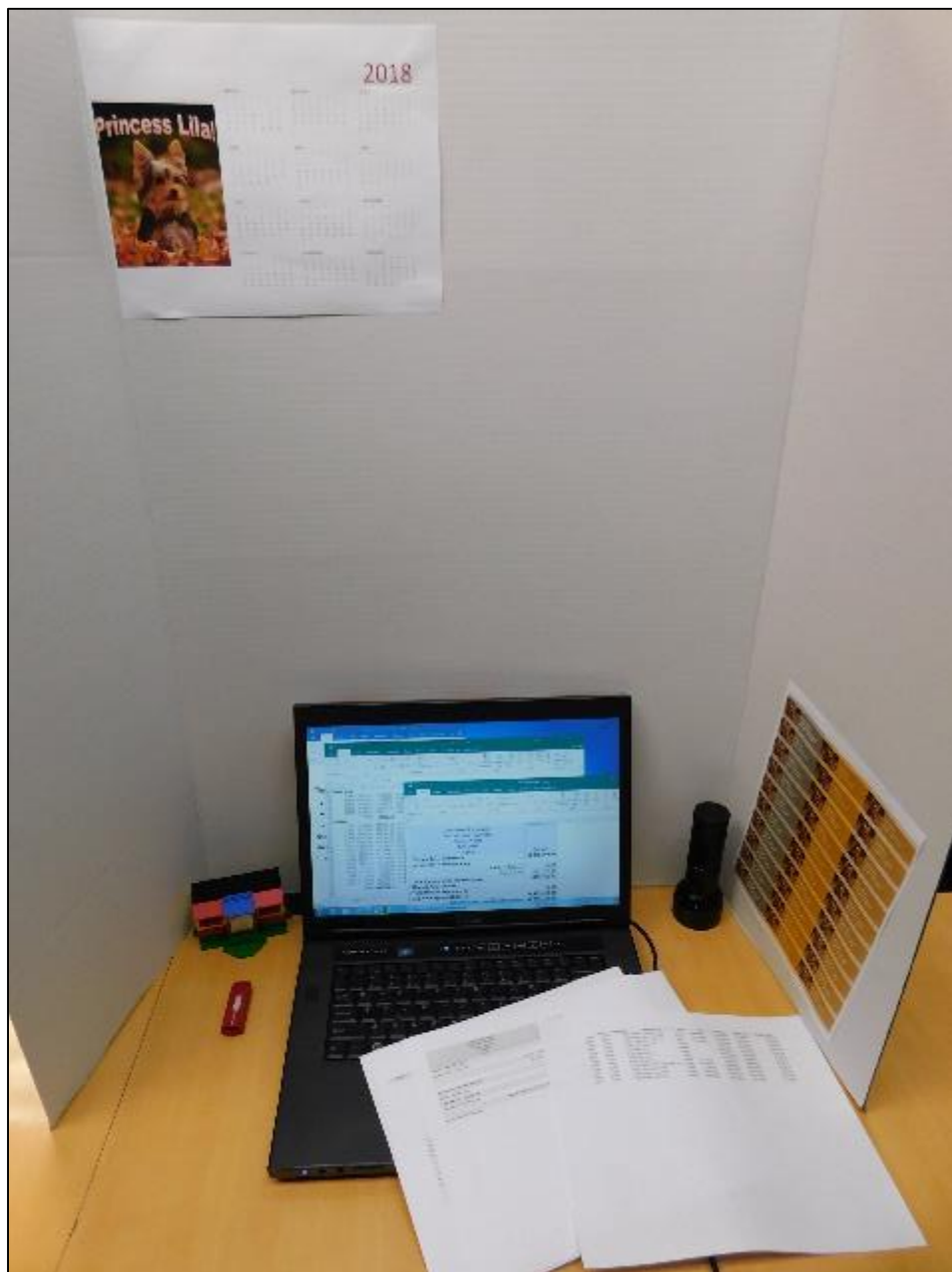




Guiding Philanthropy through Technology



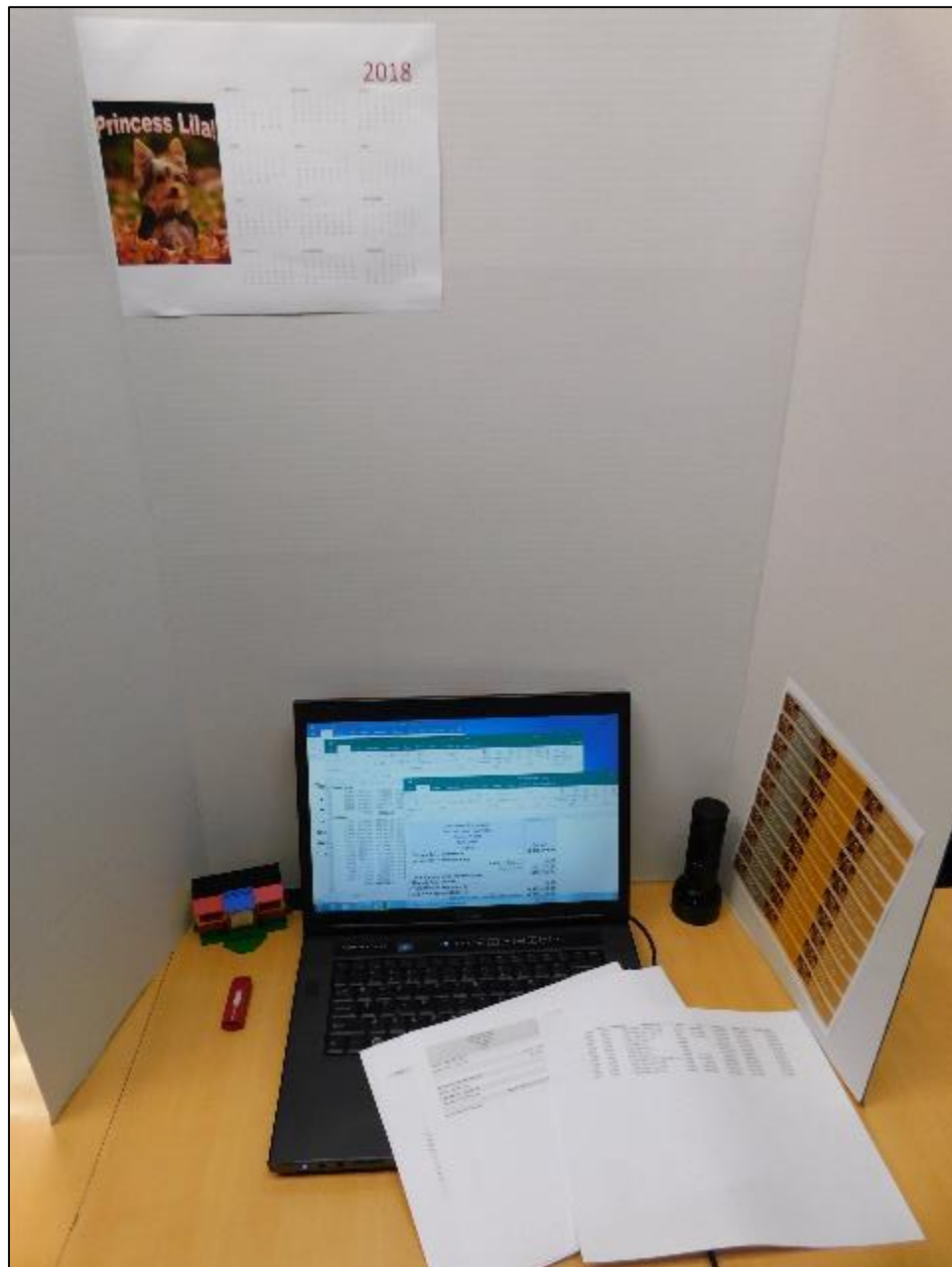
Objective 1: Demonstrate passwords can easily be guessed or cracked.



Stellar Technology  
Seattle, WA

Guiding Philanthropy through Technology

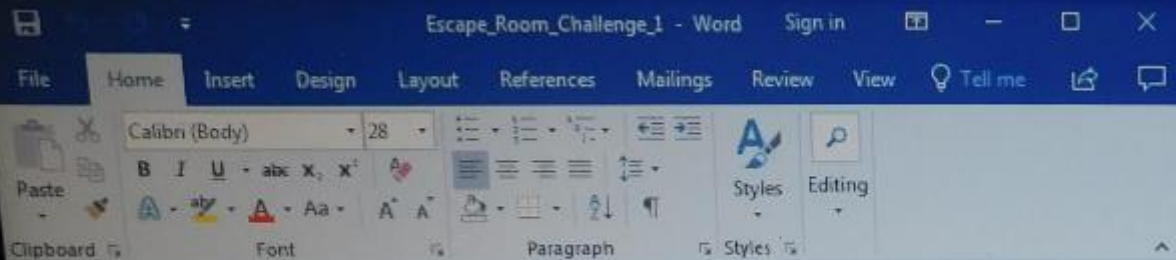




Guiding Philanthropy through Technology



Objective 2: Identify  
improperly stored PII.



There are two files on the desktop:

- Bank Rec Summary
- Bank Rec Details

Find the error in the digital files and use the PII in the printouts on the user's desk to determine the code to unlock the box!





		Donor Name	Status	Tax ID
33052	27927	13282 Be More Aware Foundation	Posted	
33067	27933	11725 Friends of the Lego Wall	Posted	73-6563483
33068	27948	21935 County Animal Rescue	Posted	74-3210509
33070	27951	14684 Victor Blackwell	Posted	74-5536783
	28040	20967 Zain Asher	Posted	
33089	31888	11706 Robin Meade	Posted	
33193		10152 Carl Azuz	Posted	
33203	31903	21888 Morris Ecure	Posted	
33204	27906	15108 Animal Shelter Fundraising LLC	Posted	xxx-xx-5589
33211	27913	12198 Olympic Committee	Posted	73-6744687
		12198 Olympic Committee	Posted	73-6744688
		11725 More Trees Please	Posted	74-3210509



Objective 3: The level of protection should be proportionate to what we are protecting





Guiding Philanthropy through Technology







Objective 4: Demonstrate compliance of physical access control policies and procedures.

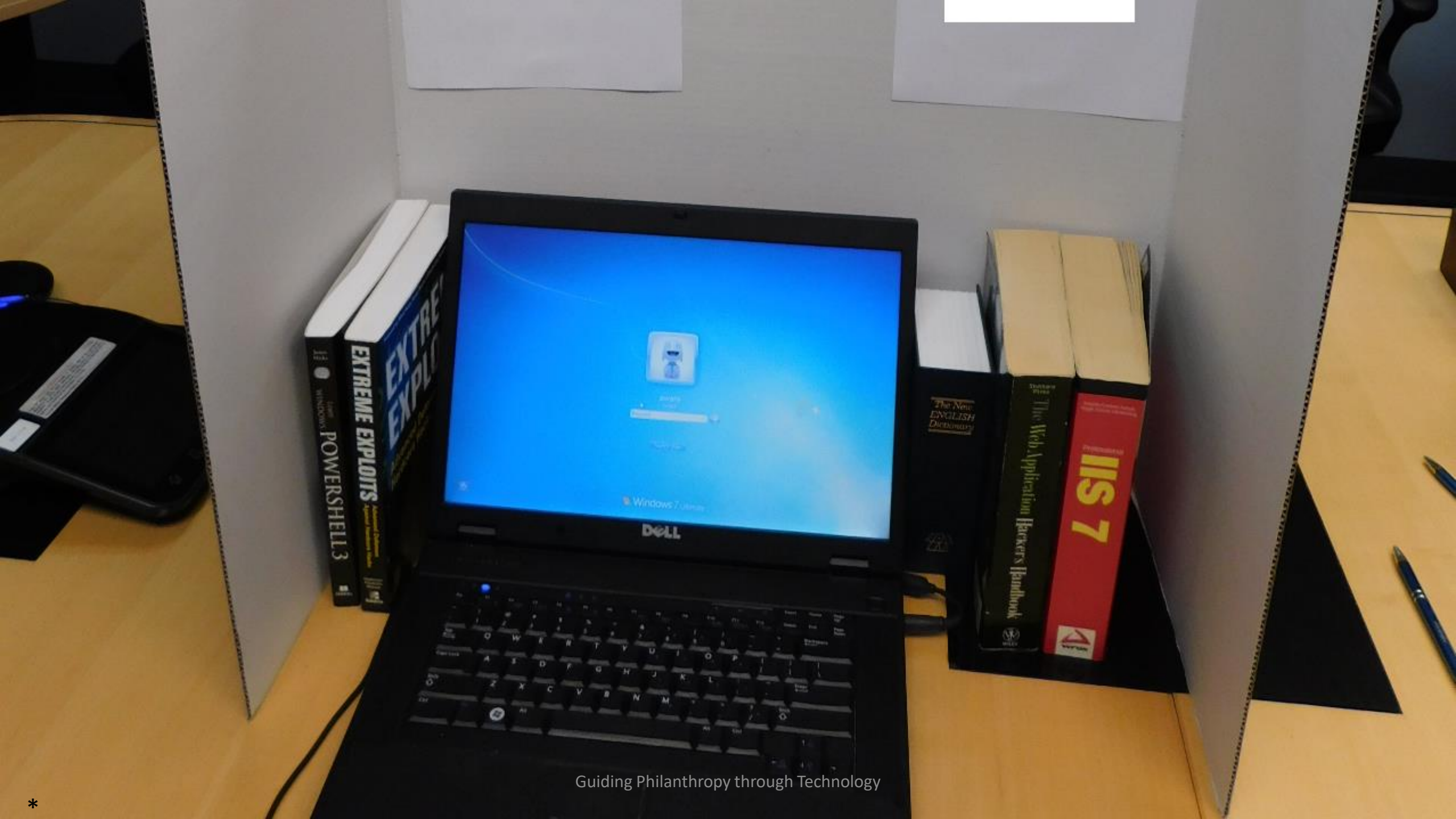


Stellar Technology  
Guiding Philanthropy through Technology

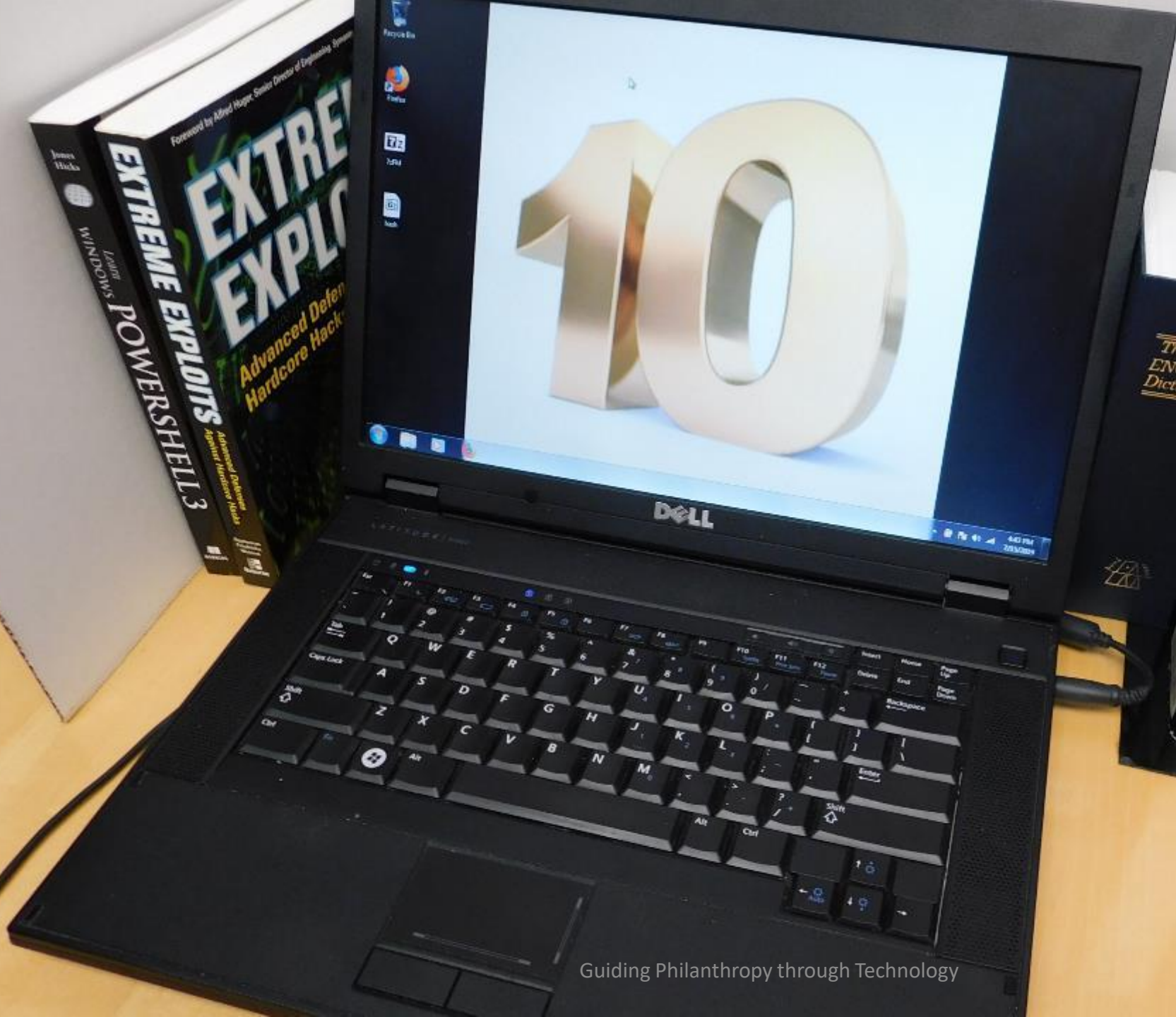




Objective 5: Recognize risk of password reuse.



Guiding Philanthropy through Technology



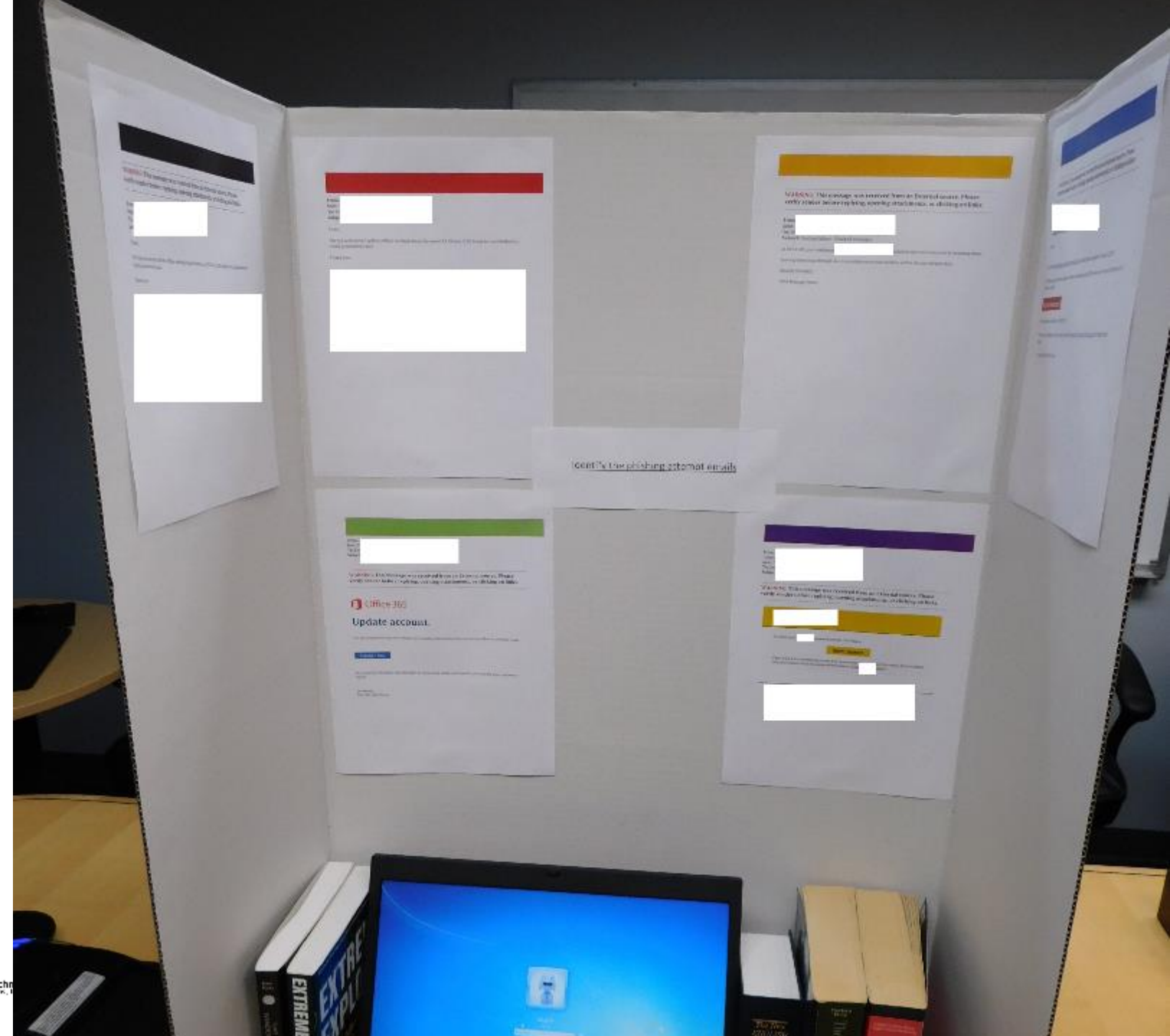
Guiding Philanthropy through Technology





## Objective 6: Identify Phishing attempt e-mails

GREEN  
~~YELLOW~~  
BLACK  
GREY  
~~RED~~  
BLUE





- Green-Y
- Black-P
- Grey-E
- Blue-B





# Objective 7: Perform a manual cipher decryption.





Offset: 10

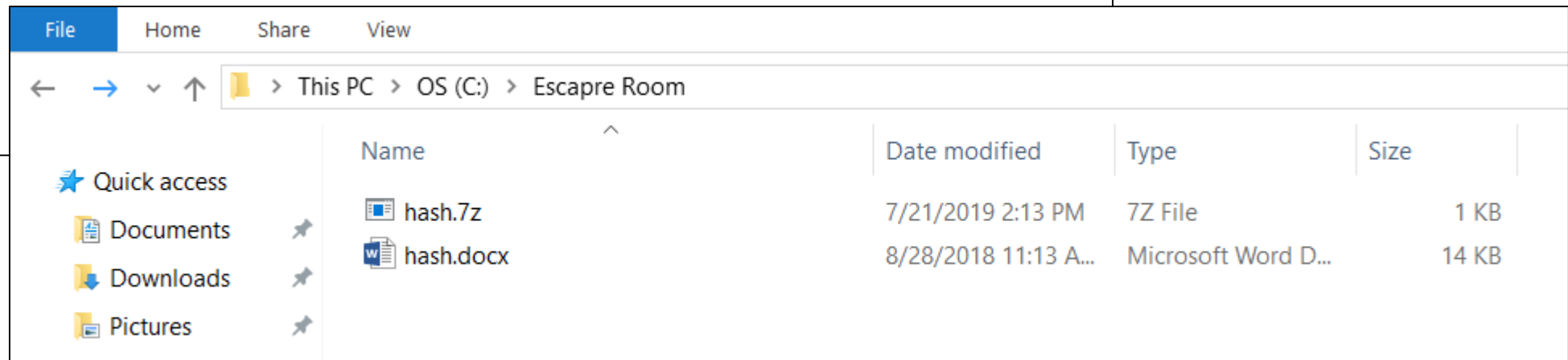
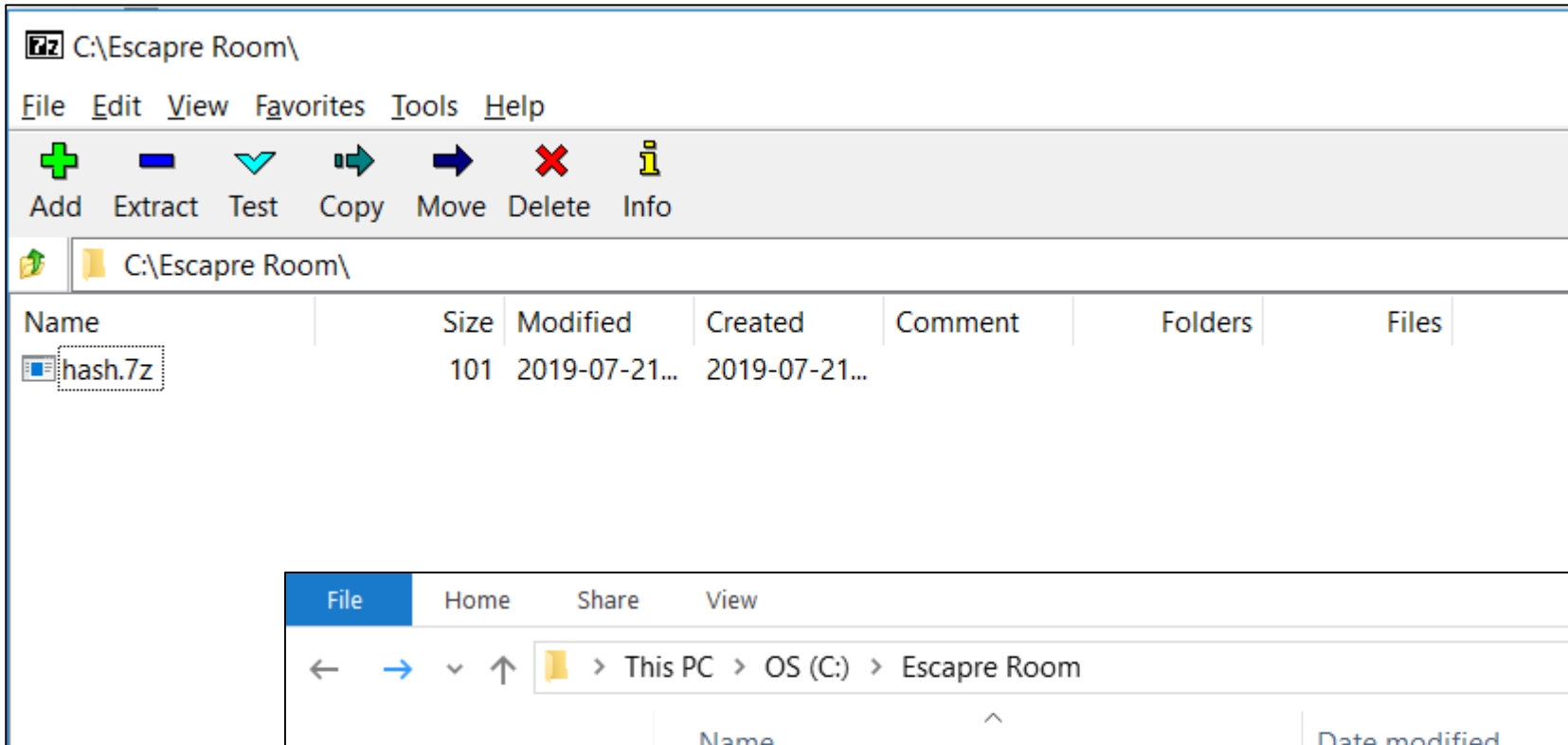
- **Green-Y=O**
- **Black-P=F**
- **Grey-E=U**
- **Blue-B=R**







Objective 8: Perform a file decryption using 7zip.



# Objective 9: Crack a hash using an online resource



0B20E35DE6FF81A819A7190DC4942C816525BDC915D11947D91E34CAA2469D86::narnia@gmail.com  
07862D2A64F3D41C460387BF78160C92886EE5621A1714DC5B3BD8D931D493A5::legomylego@yahoo.com  
1D92DAE504A70FBCAE6D3721A55D7EACAF94D3133EA5F0394B7D203D64841110::stillonaol@aol.com  
1DA9133AB9DBD11D2937EC8D312E1E2569857059E73CC72DF92E670928983AB5::fullmetaljacket@gmail.com  
A88A14ABDAB5DA4BD70E6960B01A6032C661502EA7650A2D853EBE0B3829C146::paulsimon@yahoo.com  
BF4FFB1487762665C9B10595337445BB6190D2C60B9DFE85CE68DEA4D1C4C274::masterlegobuilder@yahoo.com  
1DA9177AB9BBD11D2937EC8D1925E1E2574957059E73CC72DF92E670928983AB5::<your  
company>awareness@gmail.com  
56093992BC45C1319389321E31880279663A03F5A18C32077BF77002076C1DE3::itwasntme@compuserve.com




## Free Password Hash Cracker

Enter up to 20 non-salted hashes, one per line:

```
0CF289D2C237D4851AF3C2695AF4239CA2F4B0AEFE4EE3540E677C56FFA9EE58
D63D9A0067BDD30E49E1D194539EF68E62D6228BEDCF02EC6503DA65991BEED5
E806A291CFC3E61F83B98D344EE57E3E8933CCCECE4FB45E1481F1F560E70EB1
0B20E35DE6FF81A819A7190DC4942C816525BDC915D11947D91E34CAA2469D86
07862D2A64F3D41C460387BF78160C92886EE5621A1714DC5B3BD8D931D493A5
1D92DAE504A70FBCAE6D3721A55D7EACAF94D3133EA5F0394B7D203D64841110
1DA9133AB9DBD11D2937EC8D312E1E2569857059E73CC72DF92E670928983AB5
A88A14ABDAB5DA4BD70E6960B01A6032C661502EA7650A2D853EBE0B3829C146
BF4FFB1487762665C9B10595337445BB6190D2C60B9DFE85CE68DEA4D1C4C274
56093992BC45C1319389321E31880279663A03F5A18C32077BF77002076C1DE3
```

☐

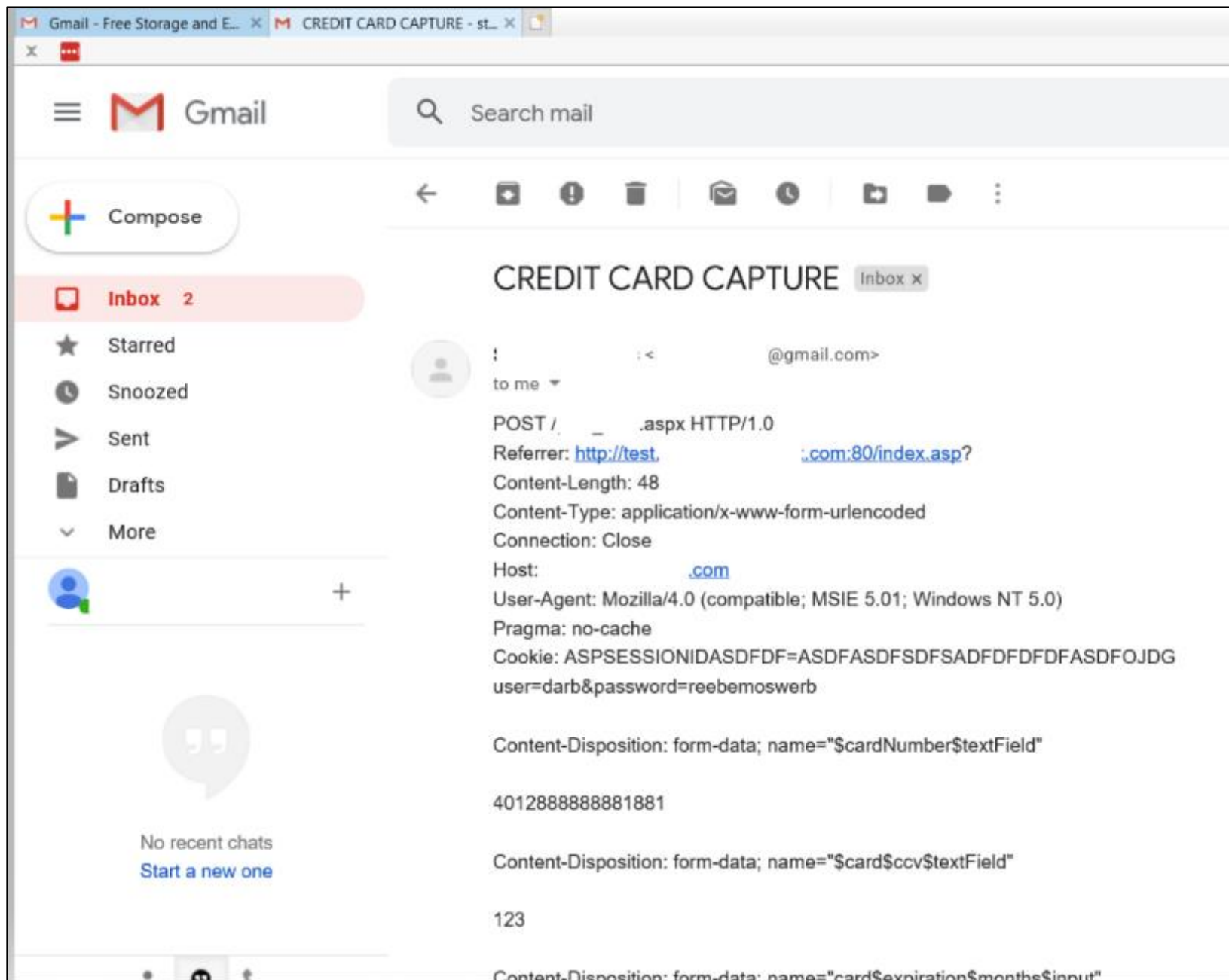
I'm not a robot

  
reCAPTCHA  
[Privacy](#) - [Terms](#)

Crack Hashes

**Supports:** LM, NTLM, md2, md4, md5, md5(md5\_hex), md5-half, sha1, sha224, sha256, sha384, sha512, ripeMD160, whirlpool, MySQL 4.1+ (sha1 sha1\_bin), QubesV3.1BackupDefaults


Hash	Type	Result
0CF289D2C237D4851AF3C2695AF4239CA2F4B0AEFE4EE3540E677C56FFA9EE58	Unknown	Not found.
D63D9A0067BDD30E49E1D194539EF68E62D6228BEDCF02EC6503DA65991BEED5	Unknown	Not found.
E806A291CFC3E61F83B98D344EE57E3E8933CCCECE4FB45E1481F1F560E70EB1	sha256	Testing
0B20E35DE6FF81A819A7190DC4942C816525BDC915D11947D91E34CAA2469D86	sha256	Password123\$
07862D2A64F3D41C460387BF78160C92886EE5621A1714DC5B3BD8D931D493A5	Unknown	Not found.
1D92DAE504A70FBCAE6D3721A55D7EACAF94D3133EA5F0394B7D203D64841110	sha256	insecure
1DA9133AB9DBD11D2937EC8D312E1E2569857059E73CC72DF92E670928983AB5	sha256	thisismypassword





Objective 10: Demonstrate methods to send sensitive information securely

Sign in to continue to Gmail



Email \*

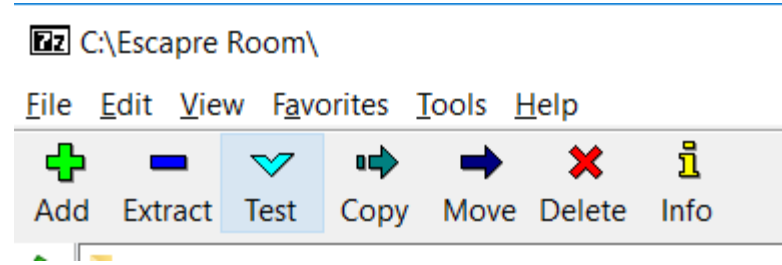

Password \*

Sign in

☒ Stay signed in [Need help?](#)

[Create an account](#)

One Google Account for everything Google



POST /lego\_refill.aspx HTTP/1.0

Referrer:

<http://test.legobrewing.com:80/index.asp?>

Content-Length: 48

Content-Type: application/x-www-form-urlencoded

Connection: Close

Host: legobrewing.com

User-Agent: Mozilla/4.0 (compatible; MSIE 5.01;

Windows NT 5.0)





# BONUS! (not really)

USB Drive left on table:

10 Minutes

Send information insecurely:

10 Minutes

# Fail!



- Remote Users
- Windows Updates
- Gmail not logged out
- Forgot to delete the decrypted 7zip file
- Forgot to empty the recycle bin
- Book safe not locked
- Prizes

# Make it your own!



- Define your objectives
- Define your teams
- Present your objectives to management
- Set your budget
- Test and test again
- Let us know how it went



Questions?