Cyber Security - It's Everyone's Responsibility

PRESENTERS: SEAN HANSON & JB WIESE, MARMOT LIBRARY NETWORK; ALYSA SELBY, BUD WERNER LIBRARY; SHANA WADE, MESA COUNTY LIBRARIES

MUG 2017 - Friday, October 6th

Bud Werner Memorial Library

Password Security

Secure

Hierarchy of Permissions

Share

Easy

useful

Hairball

Passwords

Lock Down

Home Access

Buy-in

KeePass


A 3
B 3
A 4
B 4
LastPass

“One Ring to Rule Them All”

The Master Passphrase

best colby wast boxy admix wish

6 words = 3,505 years
million years

7 words = 27

o49%^e&E%cfD%yh6

ri**ZjXR$65GI7#L

%8n*nNy^rzMwed8u

9Ge3#2vJznrgz95S

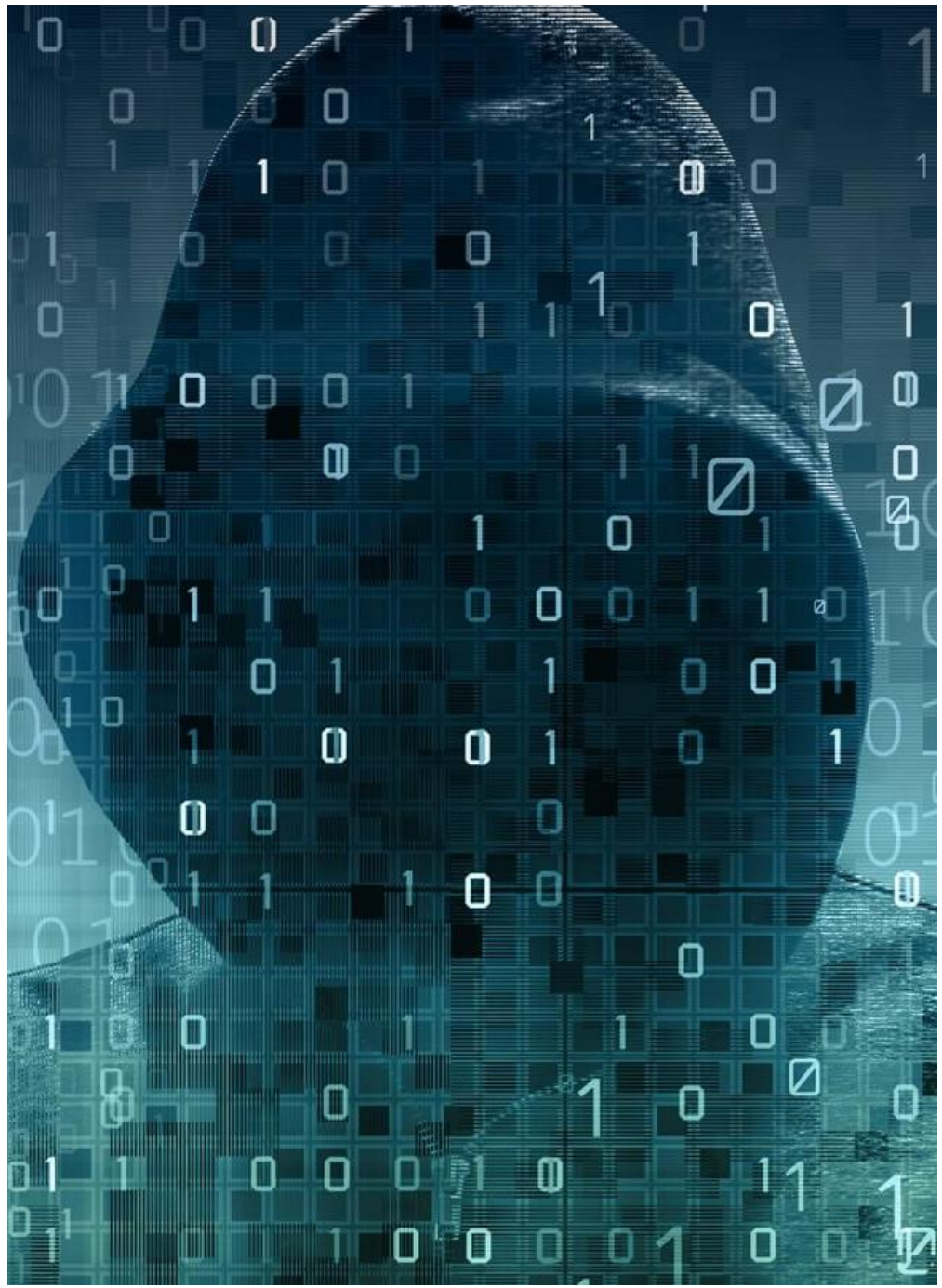
Hairball Passwords

0v1%YAZpYP3rHmJ1

K9kXc5kCm!&55S*!

^6hzI0DnC^PA@QoE

r7clJYXURPB0JYZ&



The Pyramid

- Admins (2)
- Trusted Accounts
  - Department Heads (5)
  - Support Staff with their own computers (7)
- Service Desk Staff (5 areas)

Today?

- Sierra Issue
- Still Implementing
- Review & Adopt Policies
- Force Password Changes

How Mesa County Libraries Implemented New Network and Account Security Rules


analysis

What is Privacy

ALA defines the right to privacy as ”the right to open inquiry without having the subject of one’s interest examined or scrutinized by others”

Individual security

Practical approach - Making your target smaller

Wifi

Browsers

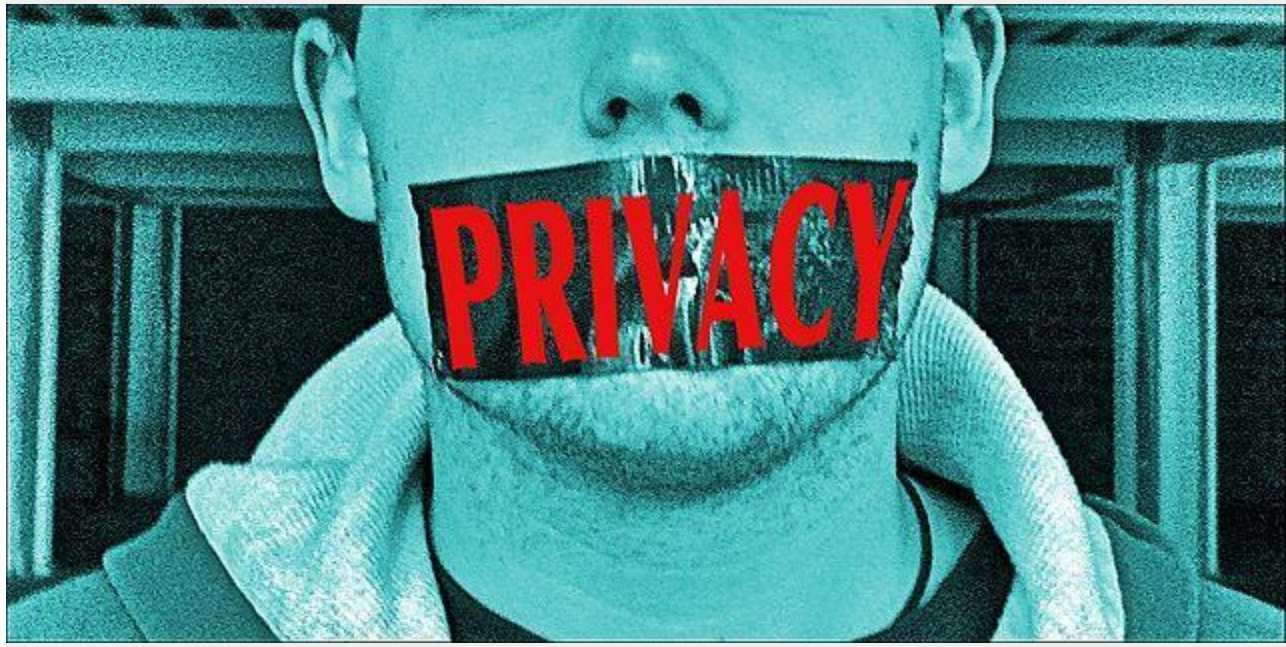
Passwords

Library Account and Password Rules

- Be complex/strong (At least 8 characters, including 1 number, 1 capital letter, and 1 symbol)
- Passwords must be unique (not used for any other system or software)
- Should a password become compromised, staff member will inform supervisor/ Associate Director immediately so the password can be reset.
- Never send passwords via email or post them on the wiki.
- Never store passwords in plain sight of unauthorized personnel, including volunteers (e.g. on monitor or under keyboard).
- Do not use the "remember me” password feature of Sierra
- Shared passwords will be reset at least every 6 months and immediately upon staff turnover.
- Managers will retain information about all systems, accounts, and locations a staff member has accessed to ensure that all the necessary passwords are changed when a staff member separates from the library. (Retain for 6 months)
- Two-step authentication may be used when available.

Sierra

Limit use and access to known work computers.



Ransonware

- Prevention is key
  - Be cautious of emails and websites/links
- Do not pay
  - It supports this type of hijacking
  - There is no guarantee you will get your files back
  - Possible further exposure or identity theft
- Only recovery is to restore from backup

Malware and Virus

- Prevention is key (see a pattern)
  - Be cautious of emails and websites/links
- Once an outbreak starts it can be very hard to contain and isolate
- User accounts with Admin privileges on multiple computers spread viruses spread very very quickly.
  - An outbreak can take 5 people working two days to clean up. (80 hours)

Questions?

- But what can I do?
  - Type website addresses in, do not use links.
  - Be very very cautious of shortened URLs
    - https://goo.gl/hFcFtU --https://marmot.org
    - https://goo.gl/XqvkMF --https://icanhazip.com
- Will these techniques work for my home computer?
- How do I know if I can trust a link or website?
- What does SSL and the padlock to the left of the URL in my web browser mean?
  - Hint just because it's encrypted with a signed certificate doesn't mean it's a trustworthy website.
- Is it safe to bank over and unsecured WiFi
  - SSL encrypts data on the user's computer and only decrypts it on the server.
  - Using any WiFi you can be the victim of a man-in-the-middle attack. More so with unencrypted WiFi because the attacker doesn't have to know the WPA2 key.
- What happens to my data on the Library public computer?
  - Does Marmot log the public's Internet.