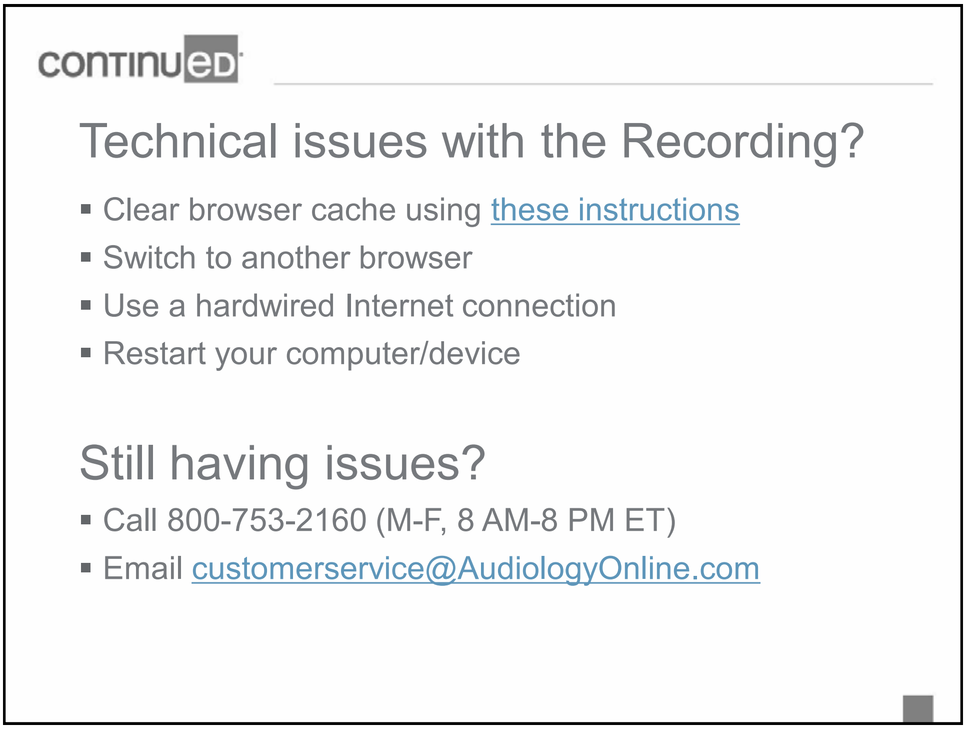
- If you are viewing this course as a recorded course after the live webinar, you can use the scroll bar at the bottom of the player window to pause and navigate the course.

- This handout is for reference only. Non-essential images have been removed for your convenience. Any links included in the handout are current at the time of the live webinar, but are subject to change and may not be current at a later date.

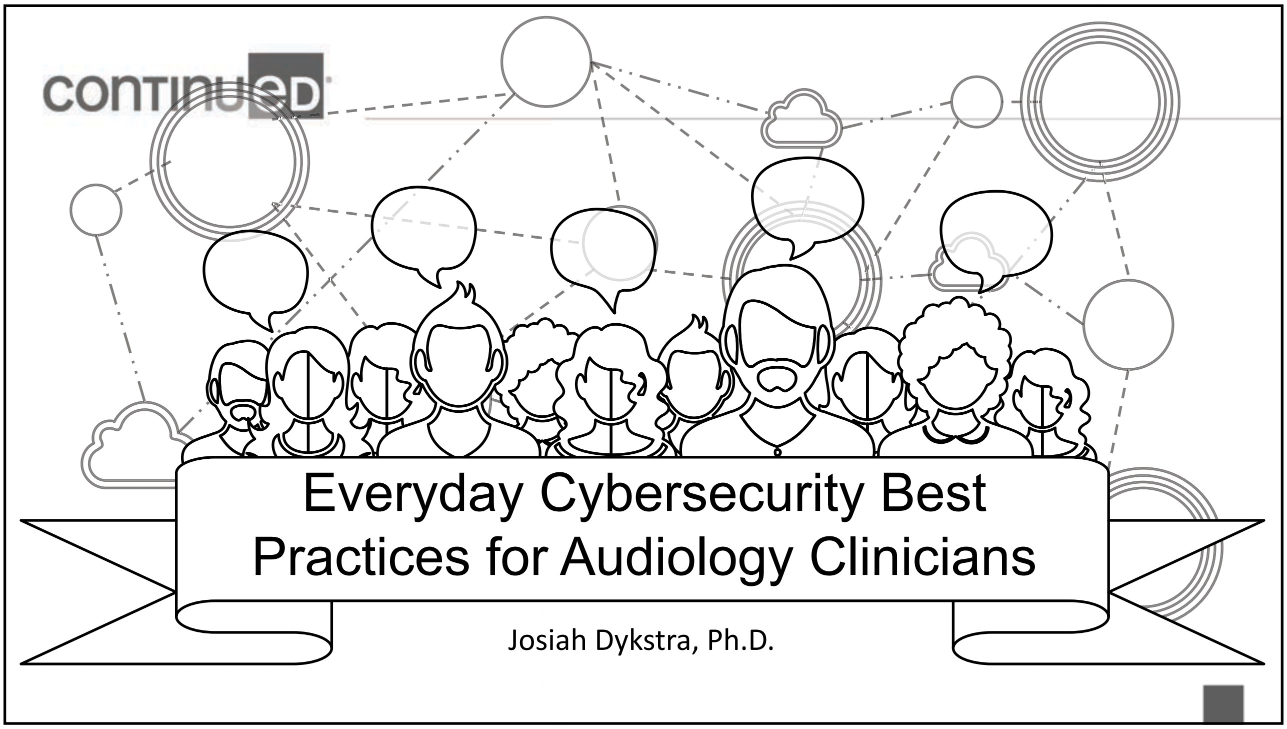


Technical issues with the Recording?

- Clear browser cache using these instructions
- Switch to another browser
- Use a hardwired Internet connection
- Restart your computer/device

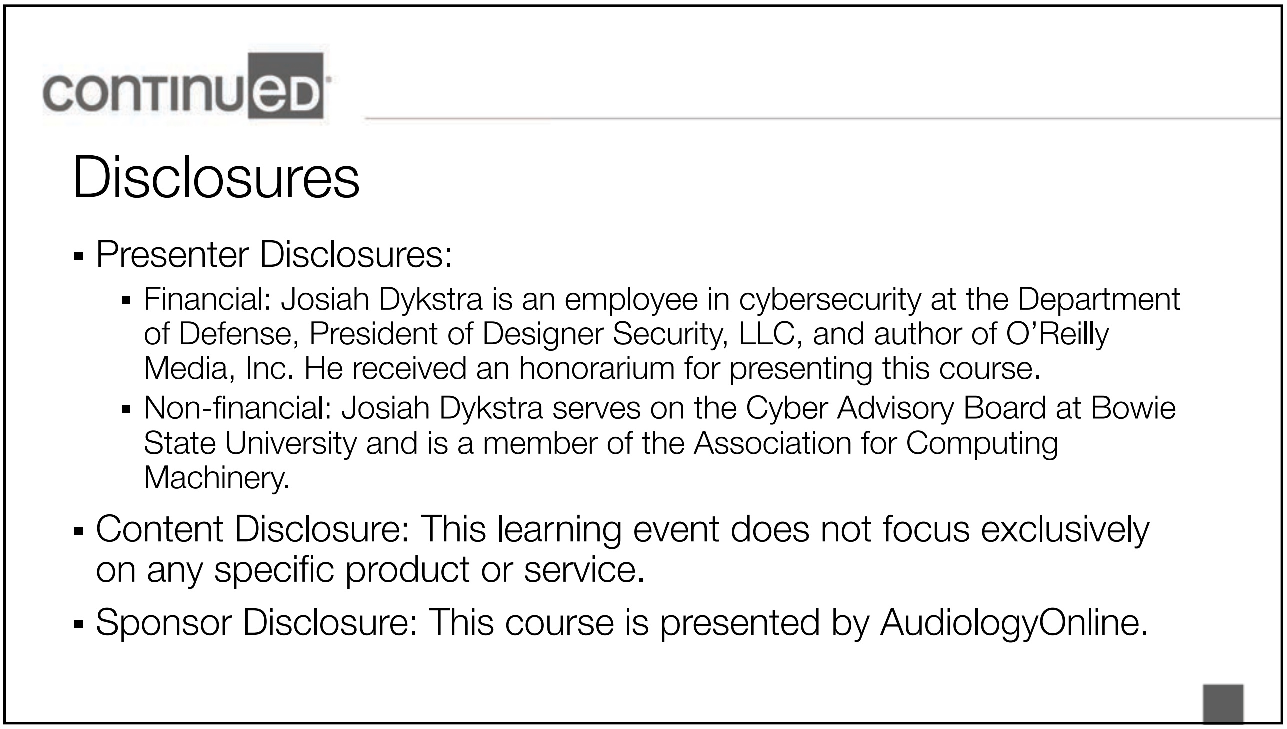
Still having issues?

- Call 800-753-2160 (M-F, 8 AM-8 PM ET)
- Email customerservice@AudiologyOnline.com



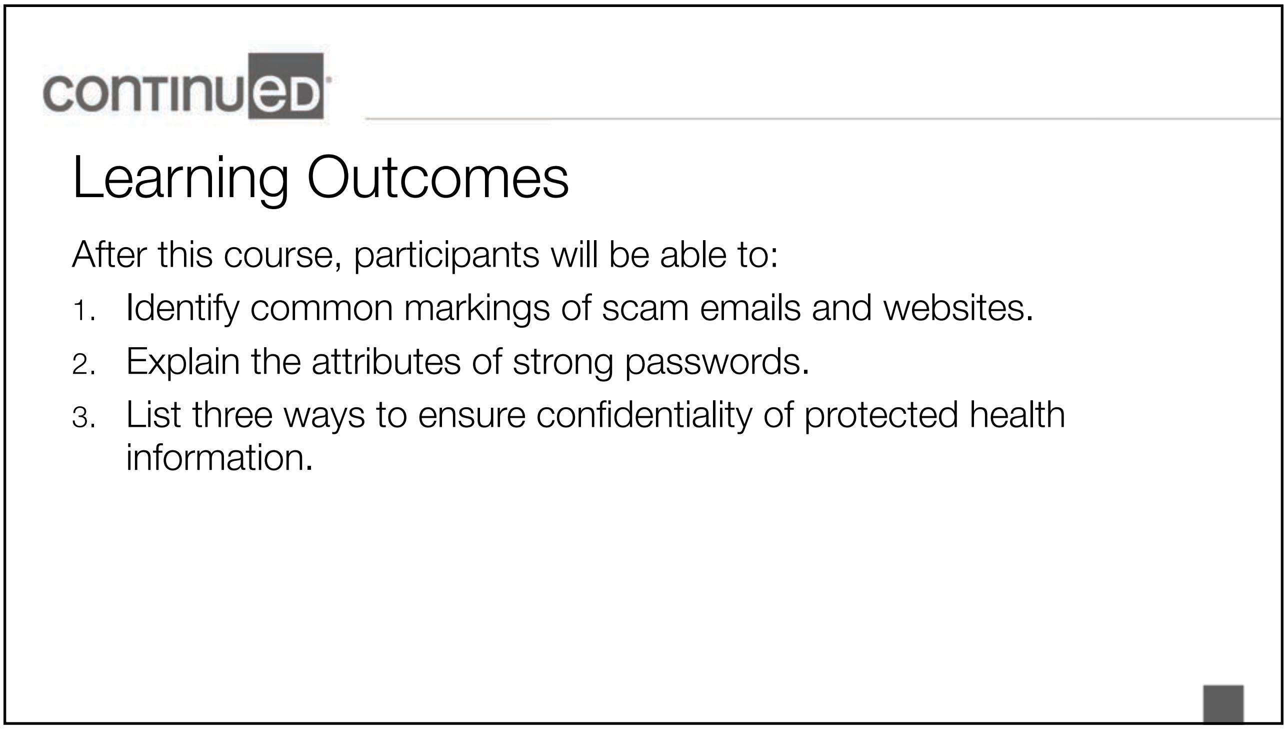
Everyday Cybersecurity Best Practices for Audiology Clinicians

Josiah Dykstra, Ph.D.



Disclosures

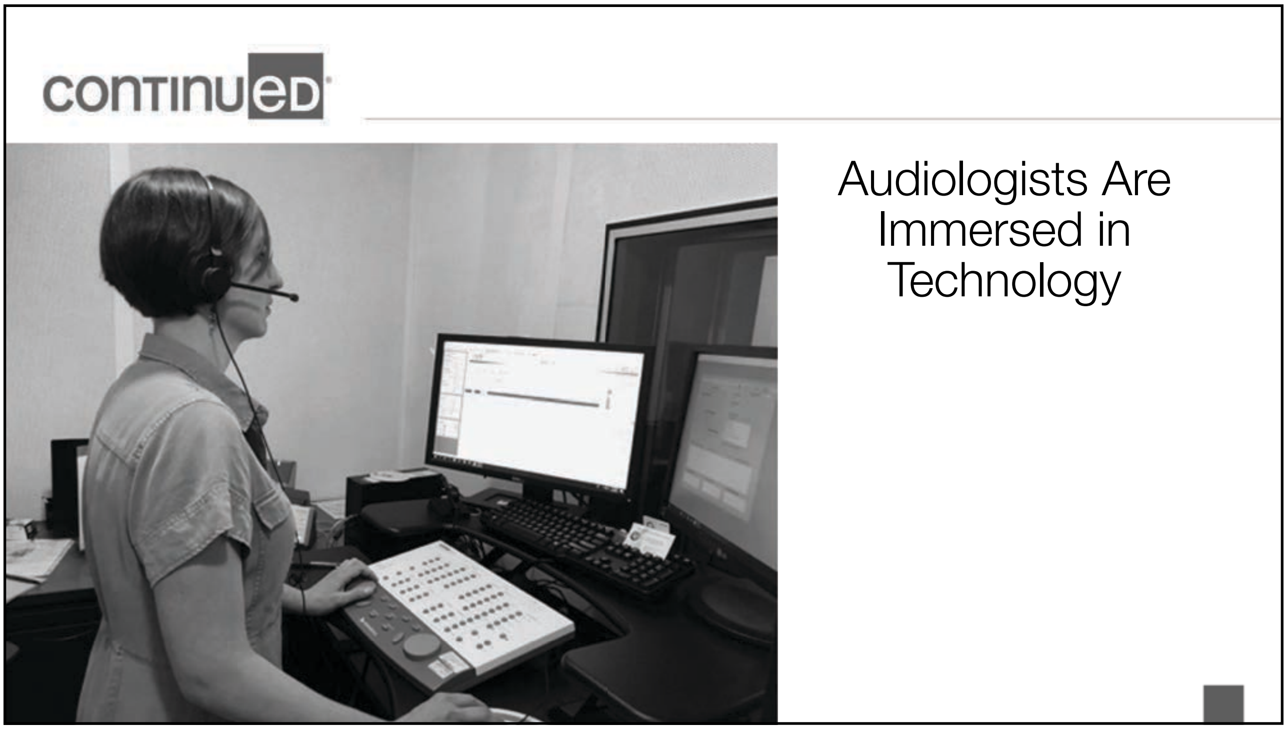
- Presenter Disclosures:
  - Financial: Josiah Dykstra is an employee in cybersecurity at the Department of Defense, President of Designer Security, LLC, and author of O'Reilly Media, Inc. He received an honorarium for presenting this course.
  - Non-financial: Josiah Dykstra serves on the Cyber Advisory Board at Bowie State University and is a member of the Association for Computing Machinery.
- Content Disclosure: This learning event does not focus exclusively on any specific product or service.
- Sponsor Disclosure: This course is presented by AudiologyOnline.



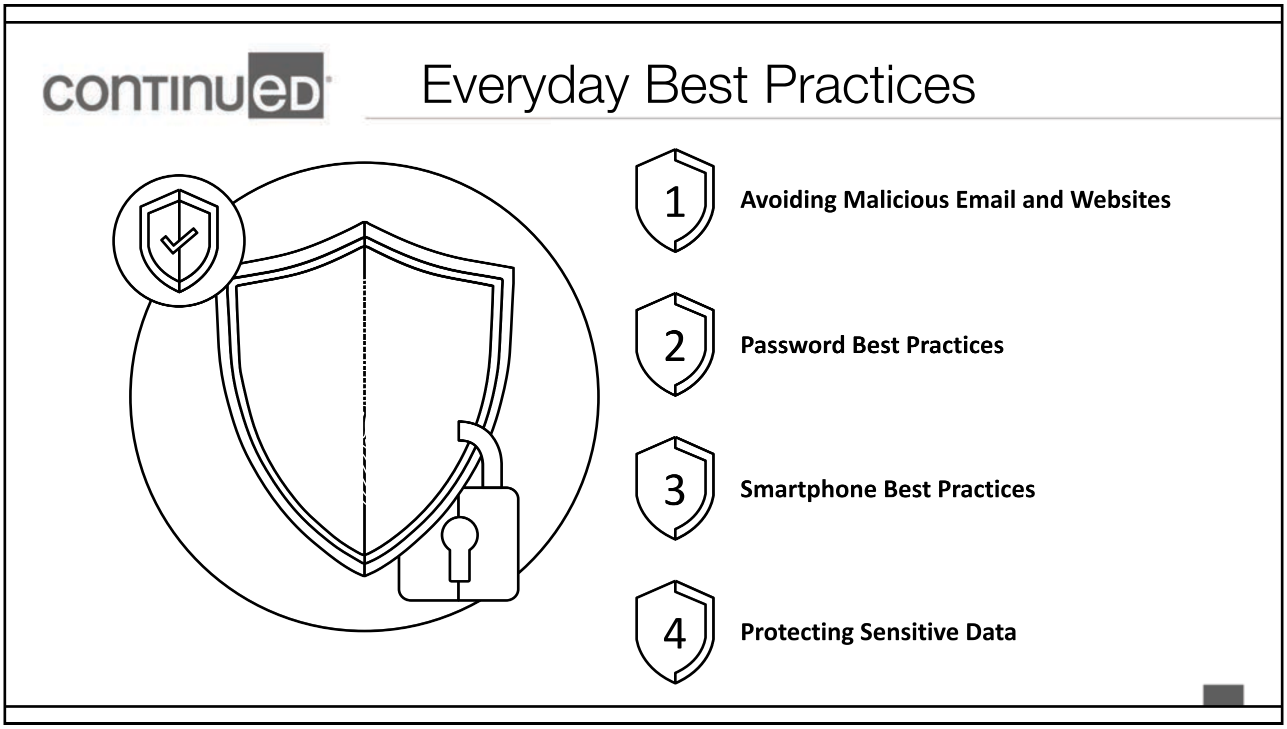
Learning Outcomes

After this course, participants will be able to:

1. Identify common markings of scam emails and websites.
2. Explain the attributes of strong passwords.
3. List three ways to ensure confidentiality of protected health information.



Audiologists Are Immersed in Technology



Everyday Best Practices

1 **Avoiding Malicious Email and Websites**

2 **Password Best Practices**

3 **Smartphone Best Practices**

4 **Protecting Sensitive Data**

continuED

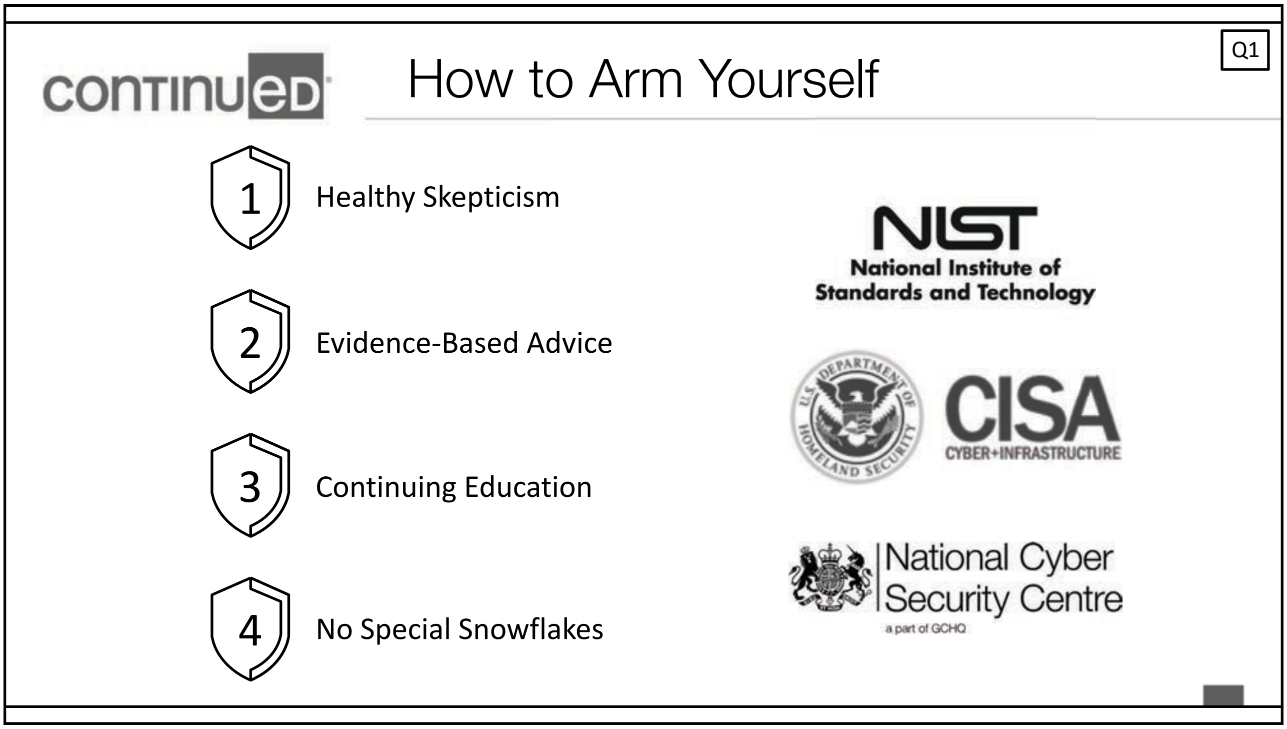
“Best Practices?”

Q2

continuED

Common Misconceptions

“We have a firewall. Our data is protected.”
“Nobody can figure out my password.”
“I will know if my computer is infected.”
”Cybersecuity is expensive and difficult to use.”
“Compliance is a sufficient security strategy.”



continuED

How to Arm Yourself

Q1

1 Healthy Skepticism

2 Evidence-Based Advice

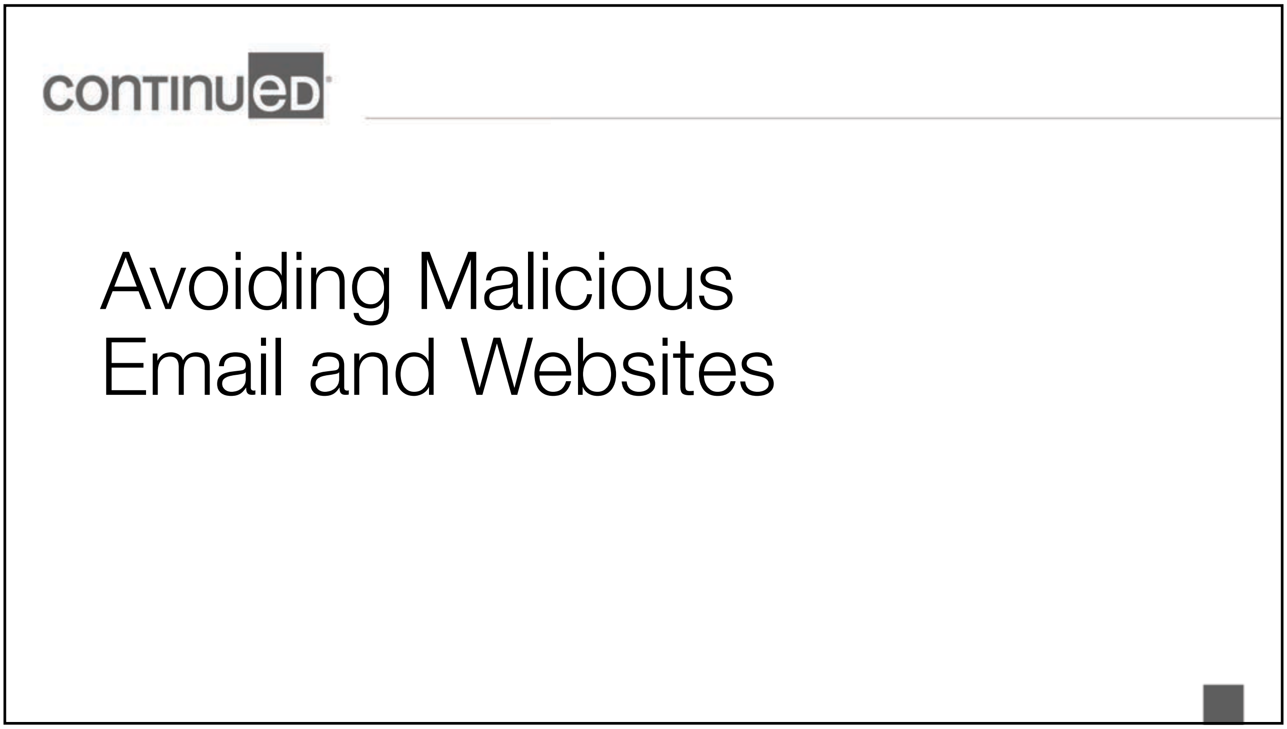
3 Continuing Education

4 No Special Snowflakes

NIST
National Institute of Standards and Technology

CISA
CYBER+INFRASTRUCTURE

National Cyber Security Centre
a part of GCHQ

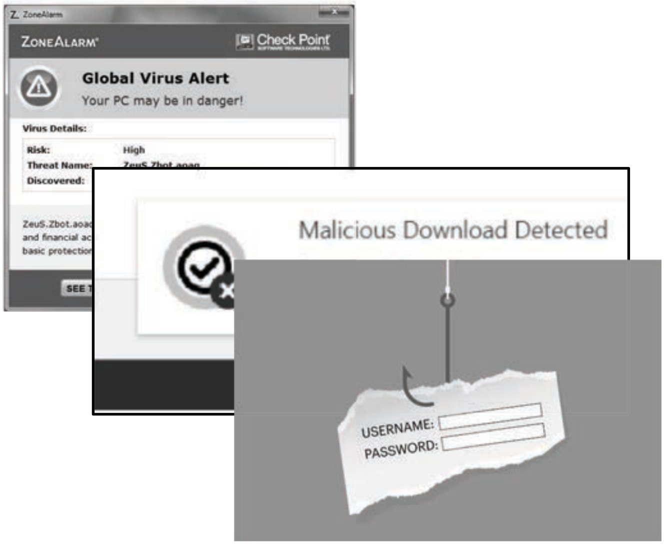


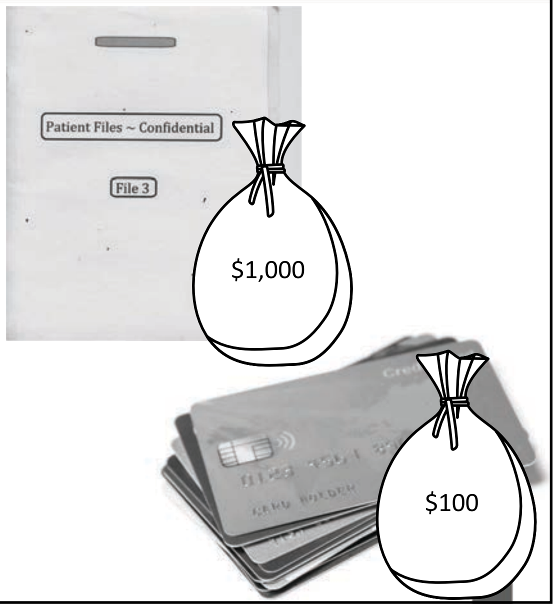
continuED

Avoiding Malicious Email and Websites

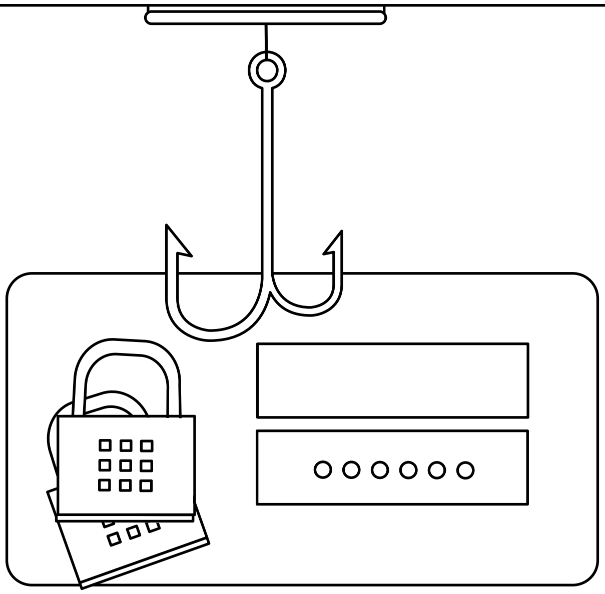
Q3

Avoiding Malicious Email and Websites





Responding to Scams



Email Scams

Do not respond!

Report messages as spam or phishing.

Use care in giving away your address.

Treat links and attachments with caution.

Have layered protection (e.g. antivirus).

Web Scams

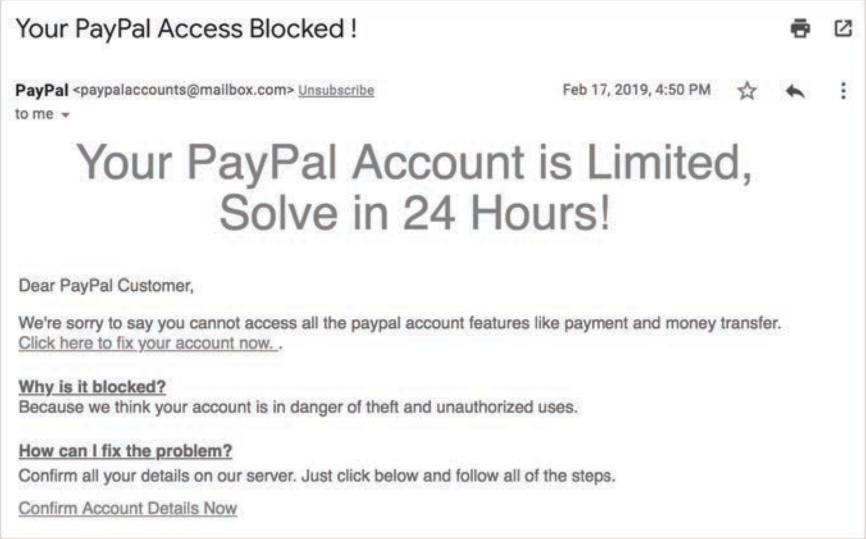
Walk away!

What did you submit?

Change your passwords.

Scan your computer for viruses.

Anatomy of a Phishing Email



Your PayPal Access Blocked !

PayPal <paypalaccounts@mailbox.com> Unsubscribe Feb 17, 2019, 4:50 PM

to me

Your PayPal Account is Limited, Solve in 24 Hours!

Dear PayPal Customer,

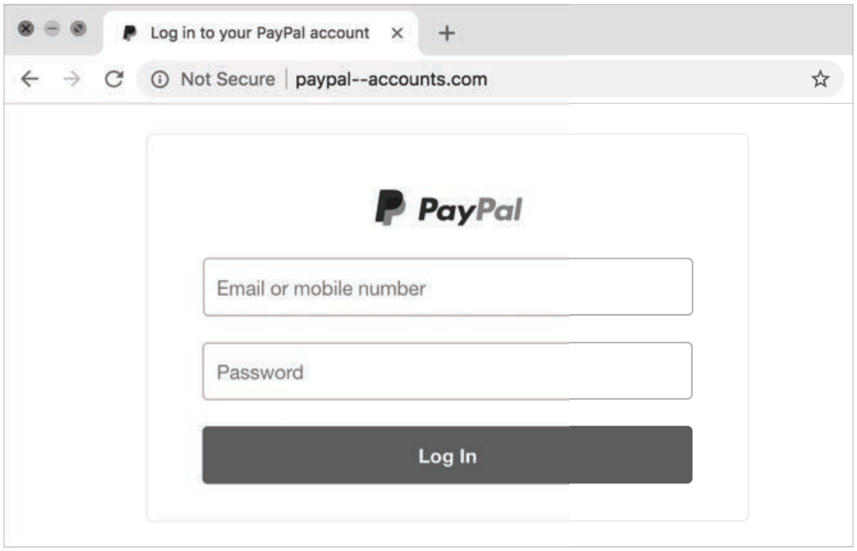
We're sorry to say you cannot access all the paypal account features like payment and money transfer. Click here to fix your account now. .

Why is it blocked?
Because we think your account is in danger of theft and unauthorized uses.

How can I fix the problem?
Confirm all your details on our server. Just click below and follow all of the steps.

Confirm Account Details Now

Anatomy of a Phishing Website

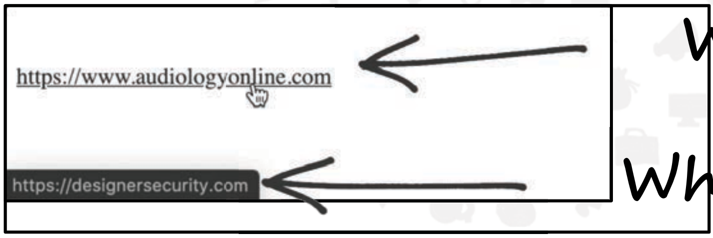


Log in to your PayPal account

Not Secure | paypal--accounts.com

More Ways to Protect Yourself

1. **Don’t click links to critical sites from email**
   If you’re suspicious about an email alert, log in to the application in your browser to ensure the request/demand is legitimate.
2. **Hover over links**
   Always hover over the URL in an email to ensure it leads to the page you expect.



https://www.audiologyonline.com

https://designersecurity.com

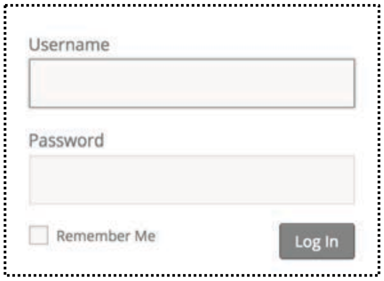
What you see

Where it goes

Password Best Practices

Password Best Practices

```
123456
12345
123456789
password
iloveyou
princess
1234567
rockyou
12345678
abc123
nicole
daniel
babygirl
monkey
lovely
jessica
654321
michael
ashley
qwerty
111111
iloveu
000000
michelle
tigger
sunshine
chocolate
password1
soccer
anthony
friends
butterfly
```

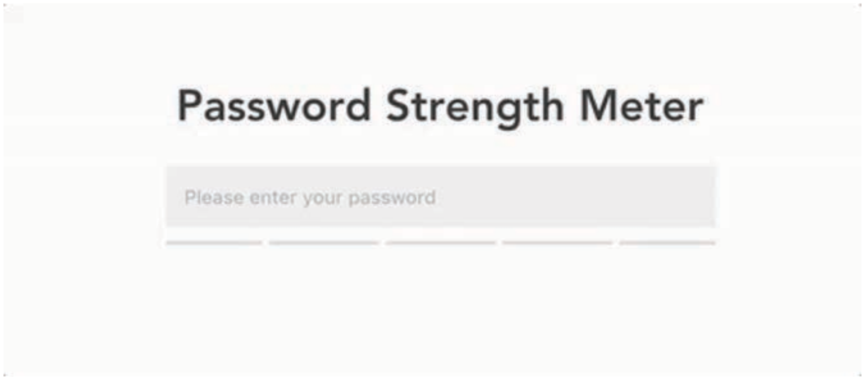


Hackers try…

- Guessing common passwords
- Brute-forcing: trying all possible passwords
- Stuffing: trying one known password on other sites
- Malware: malicious software, especially keyloggers
- Phishing: user are tricked into giving away password

```
a
b
c
d
e
f
g
h
i
j
k
l
m
n
o
p
q
r
s
t
u
v
w
x
y
z
aa
ab
ac
ad
ae
af
```

”Strong” Passwords

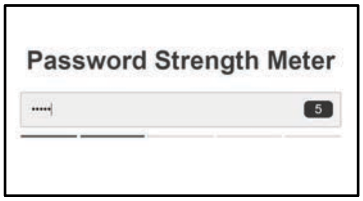


Q4 Q5 Q6

”Strong” Passwords

Strength Meters look at:

- Length
- Patterns (dictionary words, patterns, repeats, …)
- Characters (letters, numbers, capitalization, …)
- Your password history*



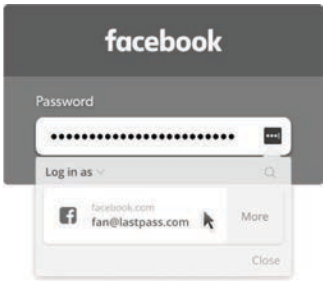
National Institute of Standards and Technology (NIST) Special Publication 800-63B

- Updated June 2017
- Widely accepted (adoption lagging for new guidance)
- No more password expirations or mandatory change
- “Easy to remember, hard to guess”

Correct-Horse-Battery-Staple-0
zebra cart slick monday
Wv%FfPM3$7kF@x#J5laP

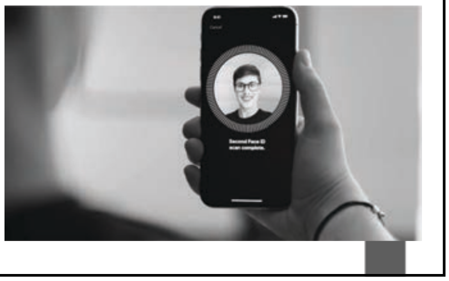
https://CorrectHorseBatteryStaple.net

The Future of Passwords



Password Managers

- Software that remembers all your passwords
- User only remembers *one* password to protect all
- Allows strong, unique passwords for every site

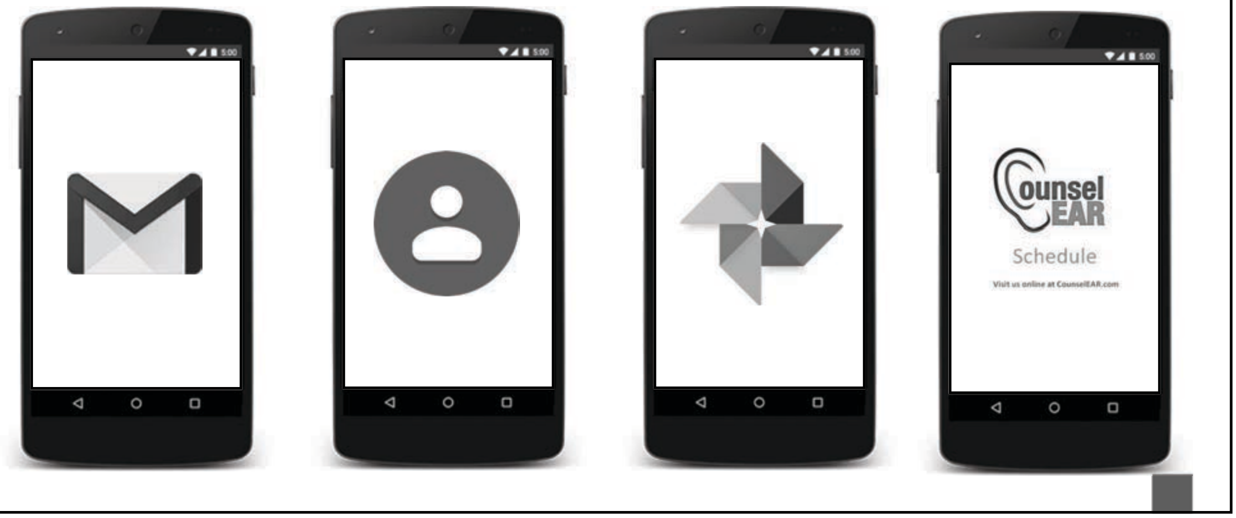


Usable or Invisible Passwords

- Human brains are bad at passwords
- We will authenticate in new ways

Smartphone Best Practices

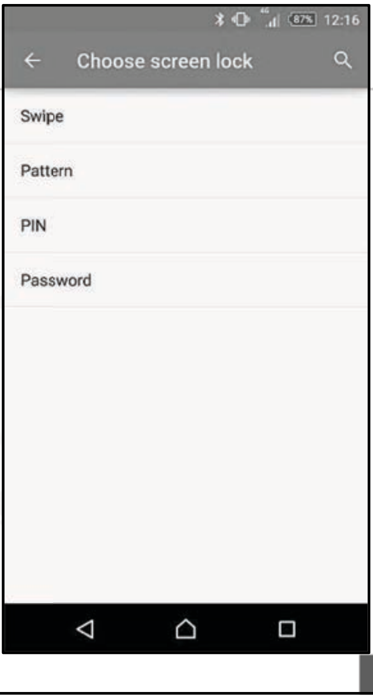
The World in Your Hands



Top 3 Best Practices

#1. Set a Screen Lock Password

Convenient to you = convenient to a thief
See previous advice about passwords
Try Face ID / Face Unlock

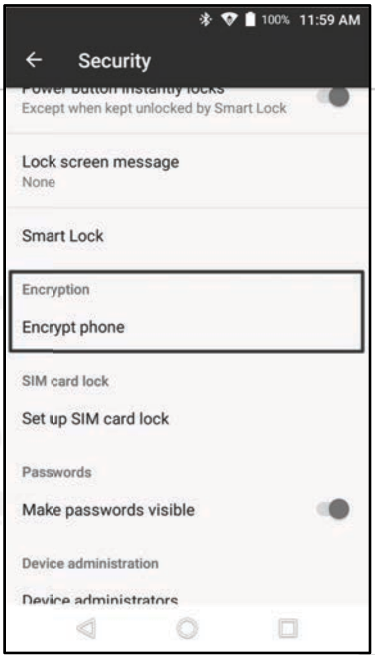


Top 3 Best Practices

#1. Set a Screen Lock Password

#2. Encrypt Your Phone

All data *on your phone* virtually unrecoverable
Enabled by default on iPhone
Android:
Settings > Security > Encrypt phone



100% 11:59 AM

Security

Power button instantly locks
Except when kept unlocked by Smart Lock

Lock screen message
None

Smart Lock

Encryption
Encrypt phone

SIM card lock
Set up SIM card lock

Passwords
Make passwords visible

Device administration
Device administrators

Q9

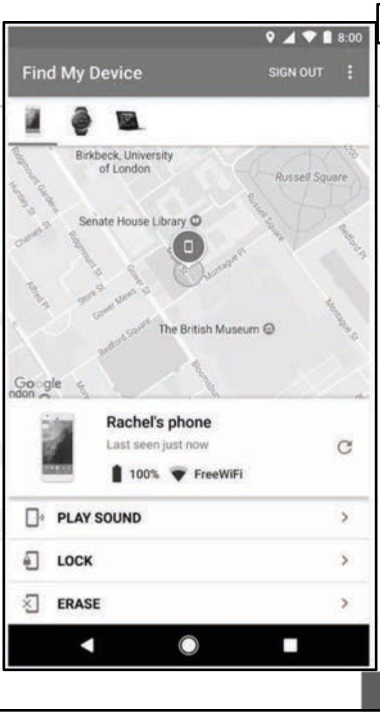
Top 3 Best Practices

#1. Set a Screen Lock Password

#2. Encrypt Your Phone

#3. Enable "Find My Device/Phone"

Get back misplaced devices
Remotely wipe the phone
Apple:
Settings > [name] > iCloud > Find My iPhone
Android:
Settings > Security > Find My Device



8:00

Find My Device SIGN OUT

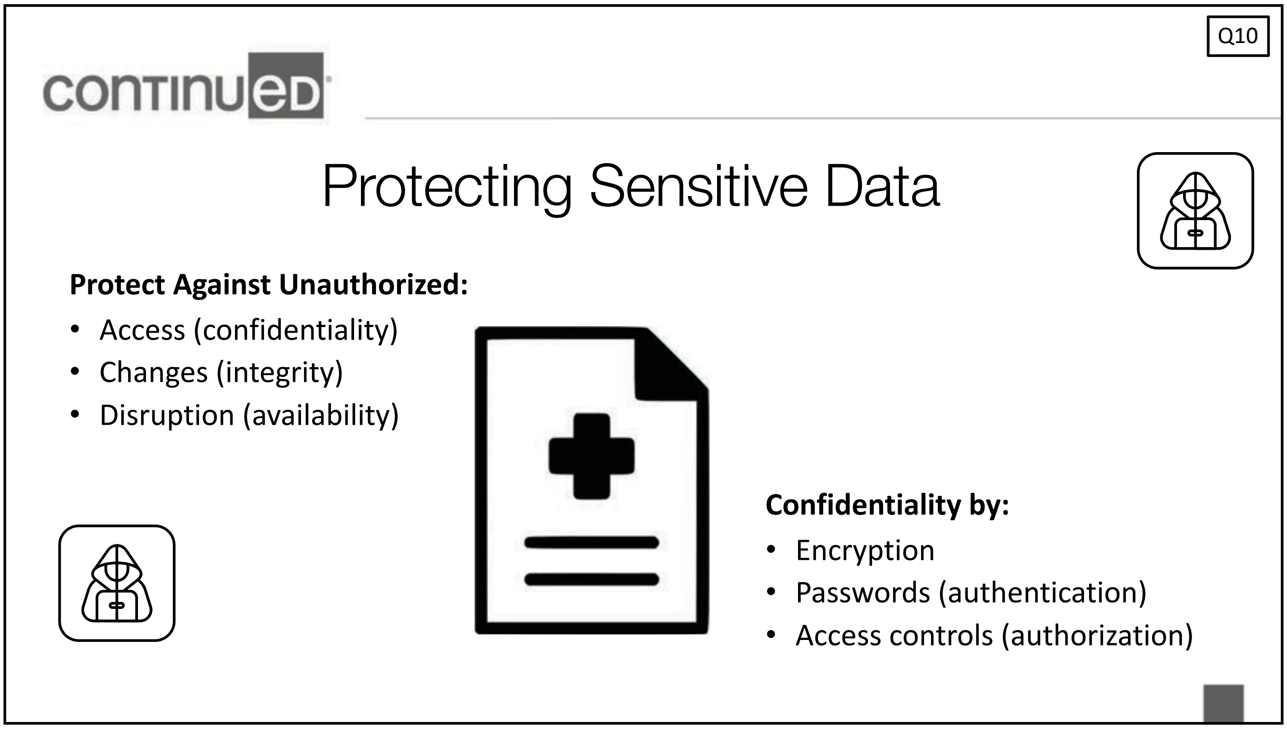
Rachel's phone
Last seen just now
100% FreeWiFi

PLAY SOUND

LOCK

ERASE

Protecting Sensitive Data



Q10

Protecting Sensitive Data

Protect Against Unauthorized:

- Access (confidentiality)
- Changes (integrity)
- Disruption (availability)

Confidentiality by:

- Encryption
- Passwords (authentication)
- Access controls (authorization)

What Can They See and Touch?

Turn off screens in photos!

Q7

Secure Communication

Most secure

United States Postal Service

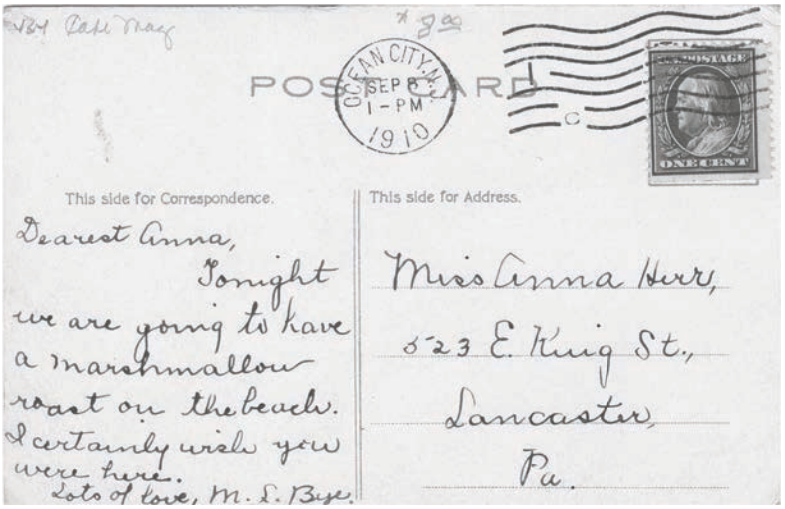
Patient Portal

Text Message

Email

Least secure

Secure Communication


Cape May

POST CARD

OCEAN CITY N.J.
SEP 6
1 - PM
1910

POSTAGE
ONE CENT

This side for Correspondence.

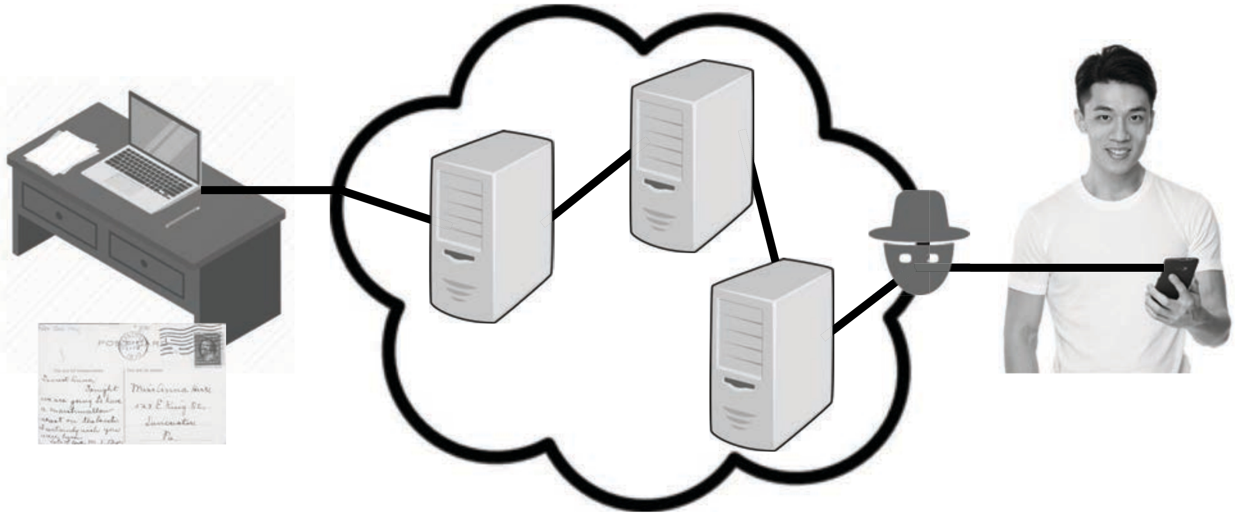
Dearest Anna,
Tonight we are going to have a marshmallow roast on the beach. I certainly wish you were here.
Lots of love, M. L. Byer.

This side for Address.

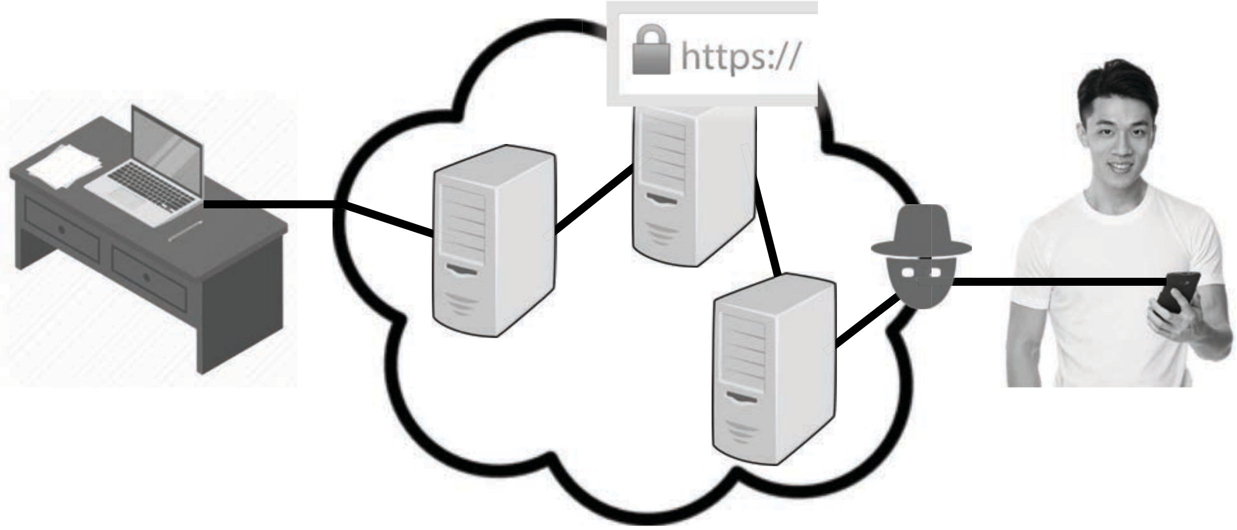
Miss Anna Herr,
523 E. King St.,
Lancaster,
Pa.

Q8

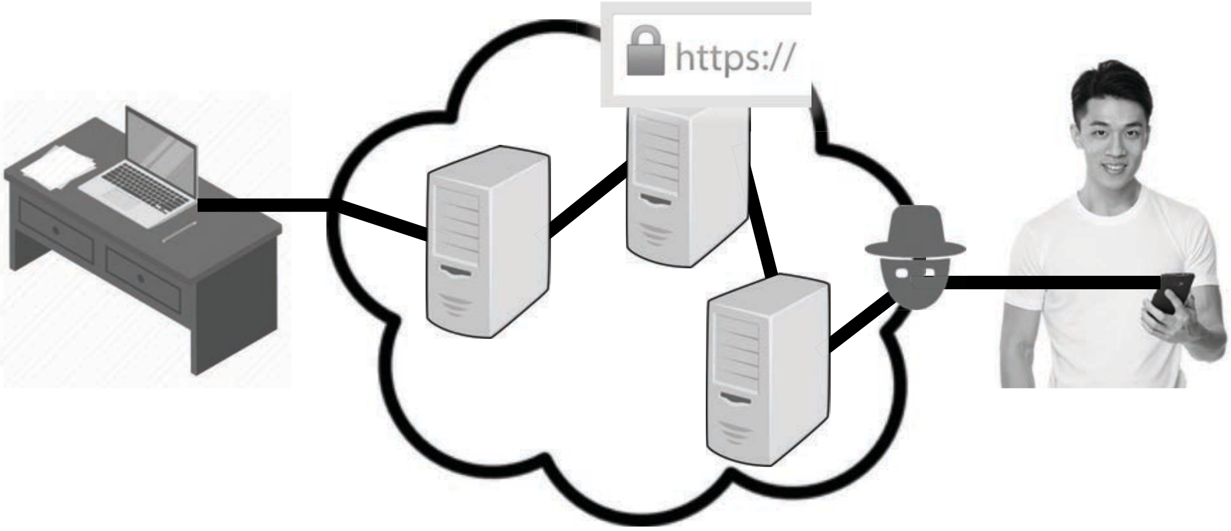
[redacted] Communication: Email



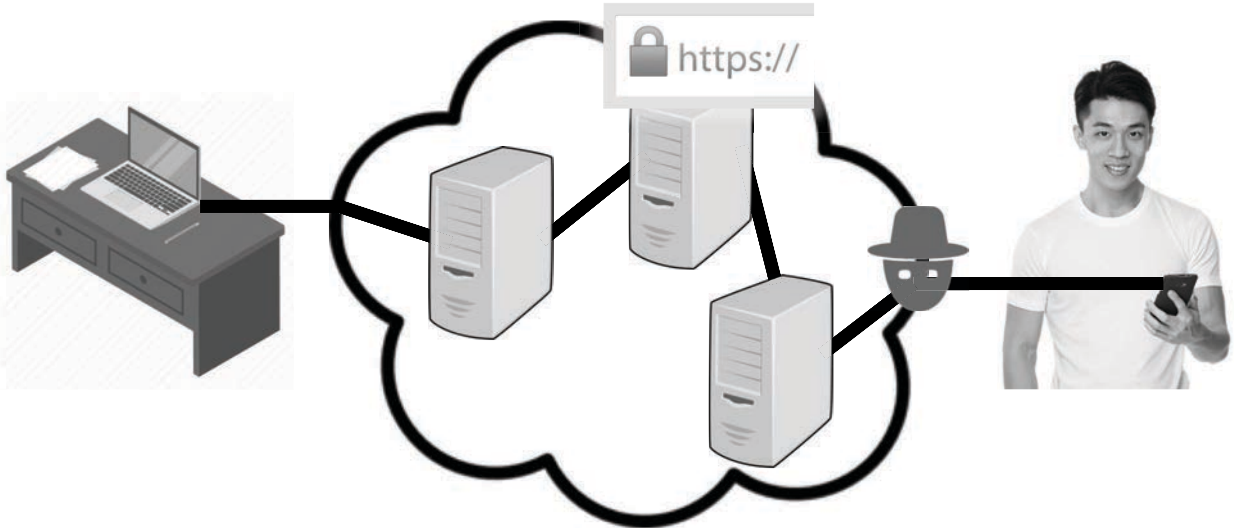
Secure Communication: Email



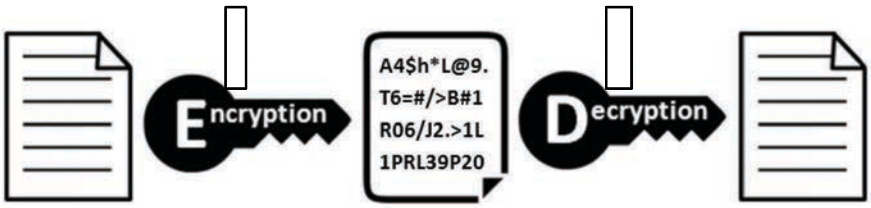
Secure Communication: Email

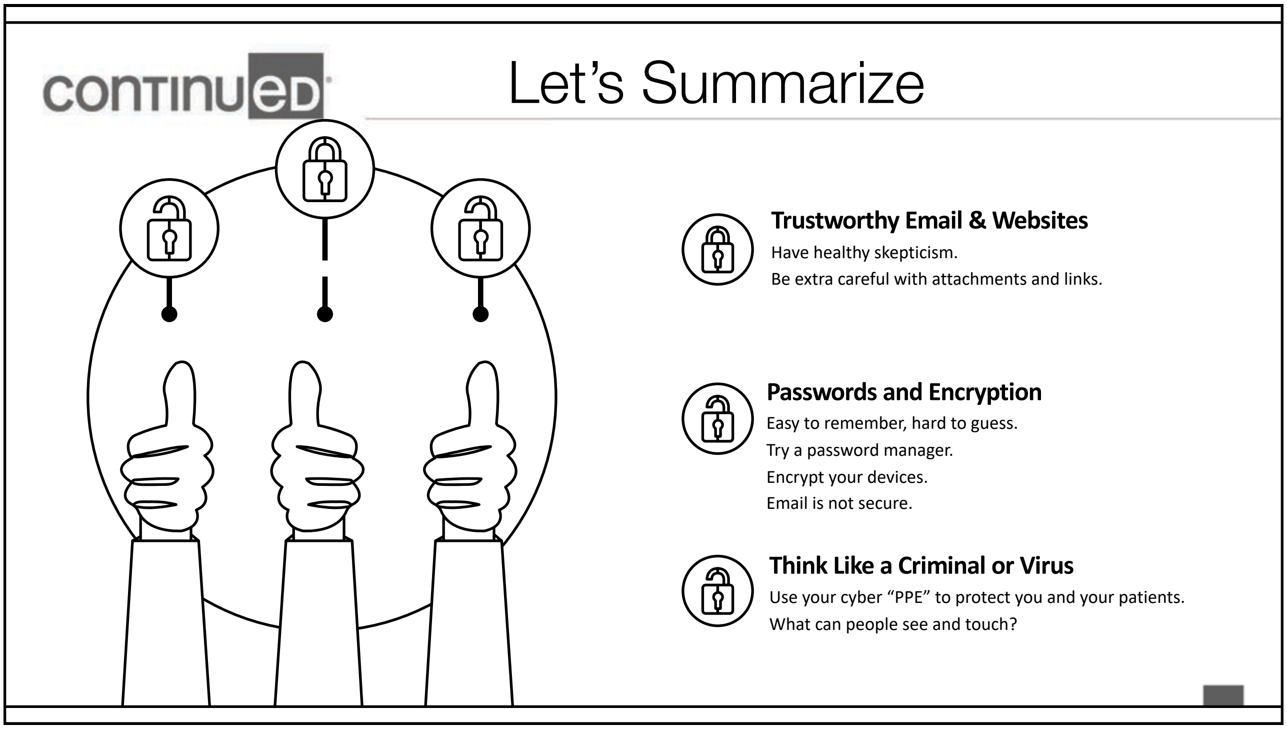


Secure Communication: Email



What is Encryption Anyway?





Let's Summarize

Trustworthy Email & Websites

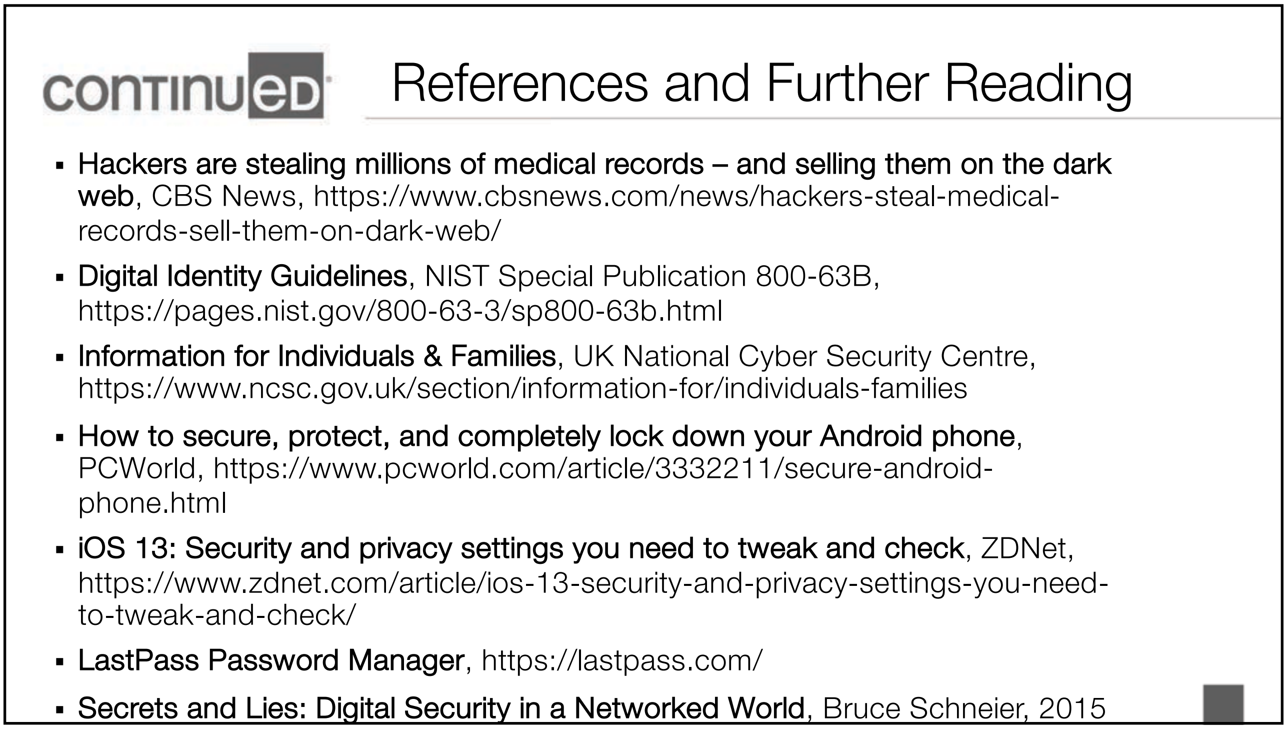
Have healthy skepticism.
Be extra careful with attachments and links.

Passwords and Encryption

Easy to remember, hard to guess.
Try a password manager.
Encrypt your devices.
Email is not secure.

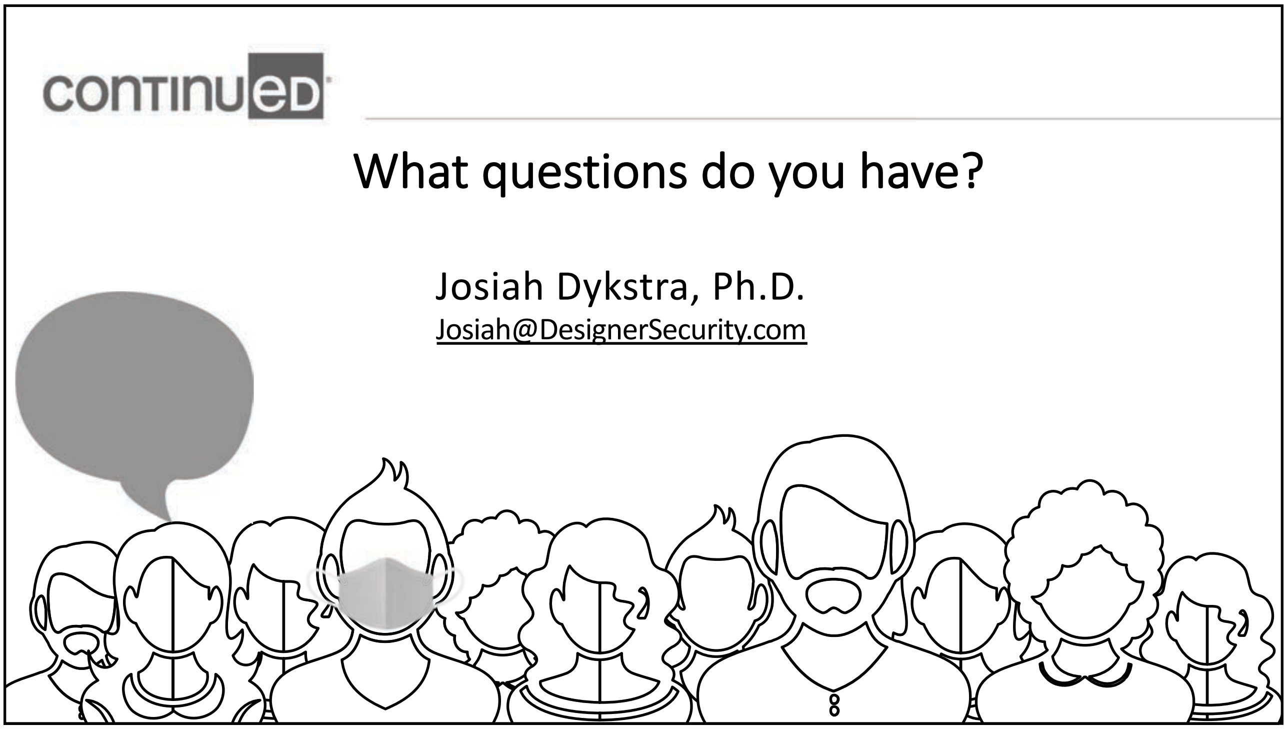
Think Like a Criminal or Virus

Use your cyber "PPE" to protect you and your patients.
What can people see and touch?



References and Further Reading

- **Hackers are stealing millions of medical records – and selling them on the dark web**, CBS News, https://www.cbsnews.com/news/hackers-steal-medical-records-sell-them-on-dark-web/
- **Digital Identity Guidelines**, NIST Special Publication 800-63B, https://pages.nist.gov/800-63-3/sp800-63b.html
- **Information for Individuals & Families**, UK National Cyber Security Centre, https://www.ncsc.gov.uk/section/information-for/individuals-families
- **How to secure, protect, and completely lock down your Android phone**, PCWorld, https://www.pcworld.com/article/3332211/secure-android-phone.html
- **iOS 13: Security and privacy settings you need to tweak and check**, ZDNet, https://www.zdnet.com/article/ios-13-security-and-privacy-settings-you-need-to-tweak-and-check/
- **LastPass Password Manager**, https://lastpass.com/
- **Secrets and Lies: Digital Security in a Networked World**, Bruce Schneier, 2015



What questions do you have?

Josiah Dykstra, Ph.D.
Josiah@DesignerSecurity.com