Protecting Yourself (and others) in a Crazy Online World

Great Western Bank®
Making Life Great®
Member FDIC

December 5, 2019

CC BY NC SA

Who am I?

- ✓ How do you know?
- ✓ How do I prove it to you?
  - ✓ Without compromising my privacy?

Identity Paradox

"On the Internet, nobody knows you're a dog."

Written by Peter Steiner and published by *The New Yorker* on July 5, 1993

© RWX Security Solutions

Who am I?

Ron Woerner, CISSP, CISM

- **Cybersecurity Professor, Bellevue University**
- **Chief Security Evangelist, RWX Security Solutions**

© RWX Security Solutions

What the $%$# are we doing here?

Agenda

- Why should I care?
- What's going on?
- Attack methods / Top issues
- Solutions
  - Awareness
  - Simple security measures
  - Protection, Detection, Response
- Where to go from here

© RWX Security Solutions

Crown Jewels

What’s most important to you?

Where is it?

How is it used?

© RWX Security Solutions

Phishing & Business Email Compromise (BEC)

MORE > NEWS > STORIES FBI Search FBI

NEWS

Stories | Videos | Press Releases | Speeches | Testimony | Podcasts And Radio | Photos | Apps

September 10, 2019

Twitter Facebook Email

Worldwide Sweep Targets Business Email Compromise

Criminal Cases Show Need to Verify Before Wiring Funds

© RWX Security Solutions

Business Email Compromise (BEC)
Email Account Compromise (EAC)

Sophisticated scams are carried out by fraudsters compromising email accounts through social engineering or computer intrusion techniques to conduct unauthorized transfer of funds.

© RWX Security Solutions

Variety of BEC

- Vendor Fraud – Invoice Payments
- Compromised or spoofed email accounts requesting a wire (ACH) transfer
- HR Requests
  - W2 or other PII
  - Changes to payroll

© RWX Security Solutions

How they find victims

Email Hacking

- Finding email addresses is trivial
- Inherently insecure
- Phishing, Spear Phishing, Whaling

© RWX Security Solutions

How they communicate with victims

Spoofed email:

From: john.smith@domain.com

Reply-To: bad.guy@scammer.com

Look-alike domain registered:

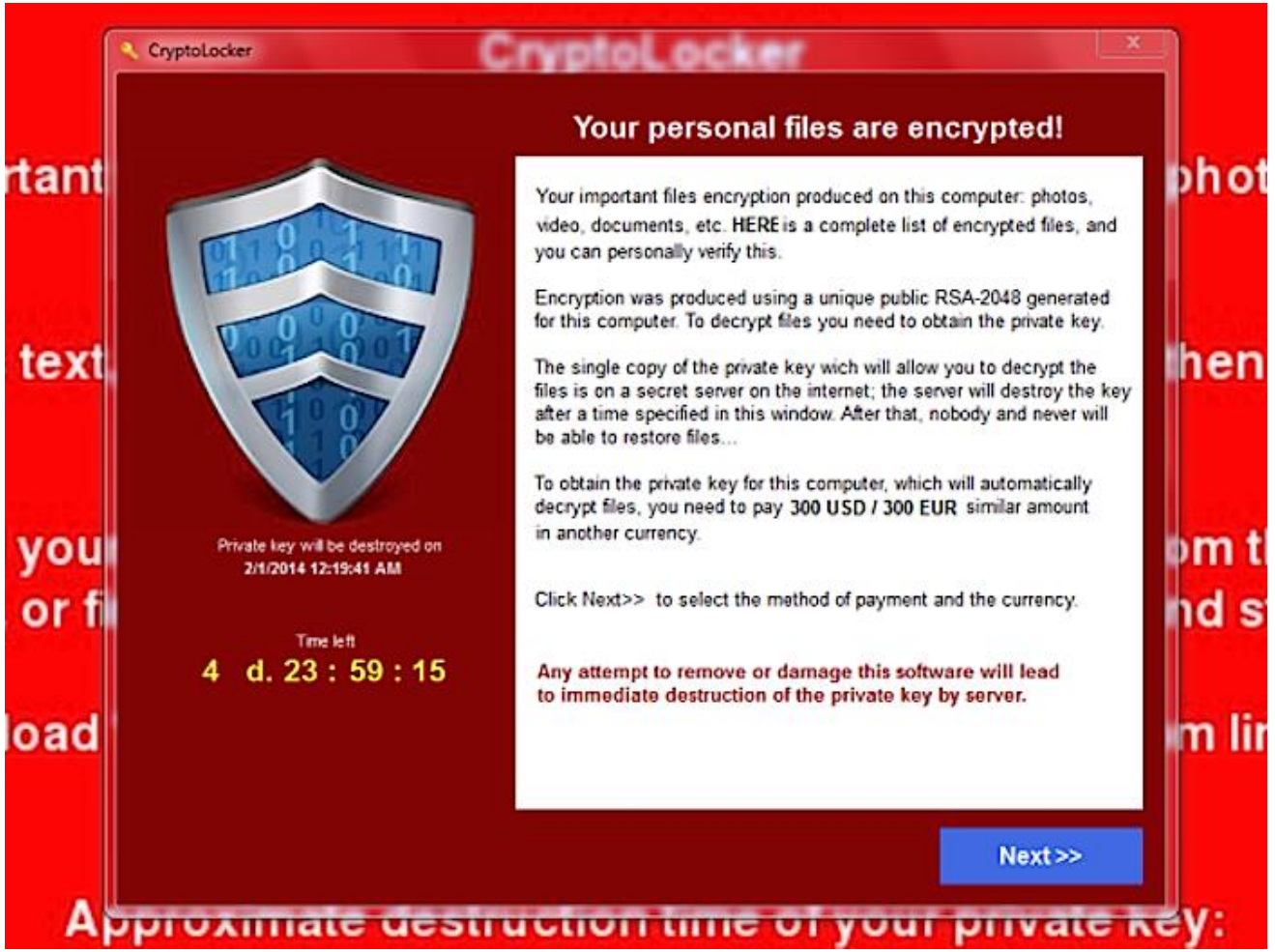
john.smith@do**m**ain.com legitimate

john.smith@do**rn**ain.com fraudulent

Compromised email account:

Phishing or malware used to steal credentials for john.smith@domain.com

Ransomware

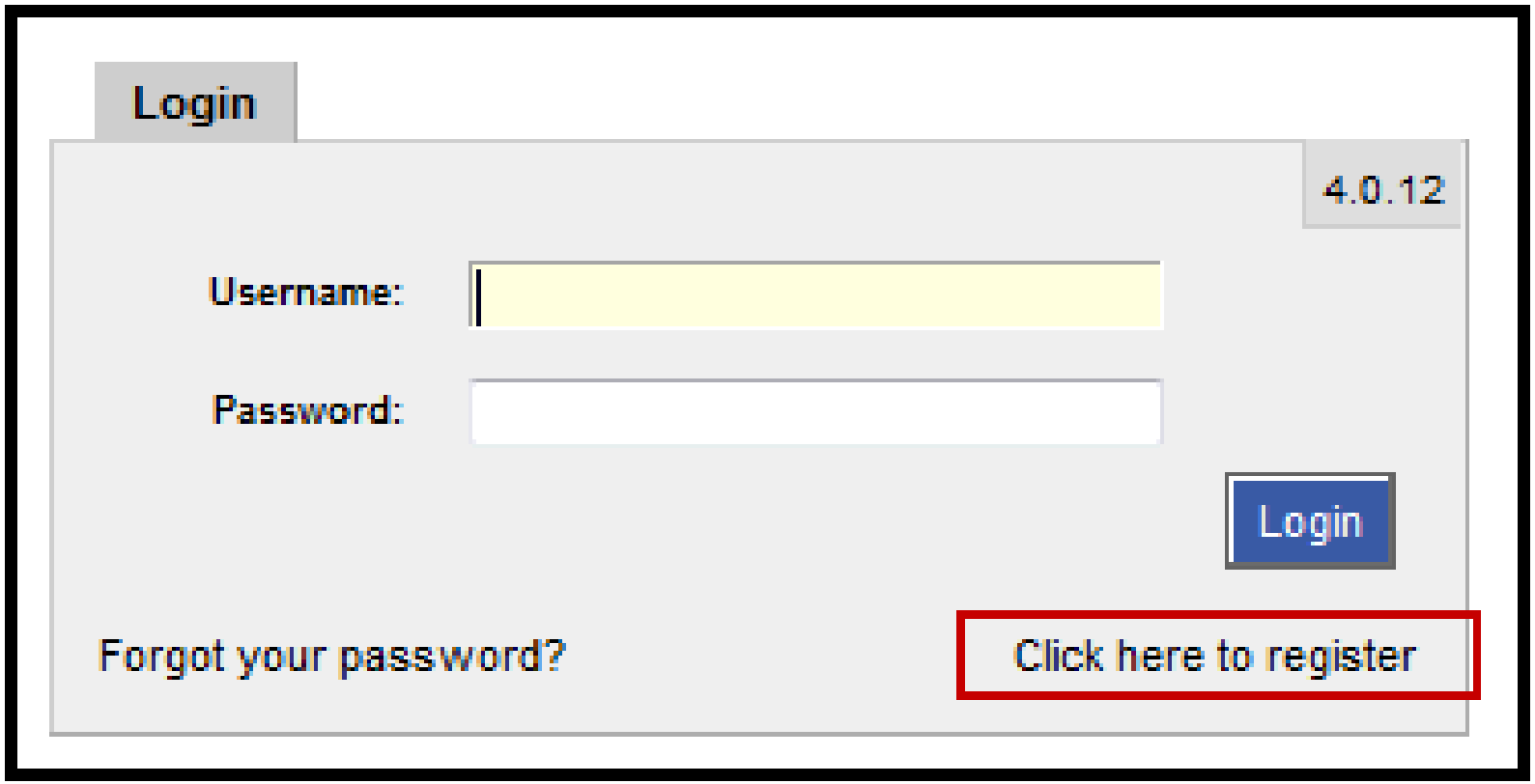


https://www.nomoreransom.org/

ran·som·ware, ransəmˌwe(ə)r/ *noun*

A type of malicious software designed to block access to a computer system until a sum of money is paid.

Stolen Credentials



© RWX Security Solutions

Required for Fraud

Dissecting the Psychology of the Wily Insider
https://www.peerlyst.com/posts/dissecting-the-psychology-of-the-wily-insider-ron-woerner

© RWX Security Solutions

What can I do?

© RWX Security Solutions

What You Can (Should) Do

Only You can Protect Yourself and Others

© RWX Security Solutions

What You Can (Should) Do

© RWX Security Solutions

Simple Steps for Cyber Security

- "Trust, but verify"
  Be a little skeptical
- Account Security
  - Multi-factor authentication
  - Password keepers
- "Be Prepared"
  - It's not if, but when…
- Updated your PC & apps
  - Pay a little now or a lot later
- Encrypt
  - Websites
  - Email
  - Databases

© RWX Security Solutions

Ransomware Defenses

- Patch - Update
- Backup data
- Active Spam & Internet Filters
- Update Anti-Virus
- Employee discretion
- Incident Response Plan

- DHS CISA: https://www.us-cert.gov/Ransomware
- CIS Facts, Threats, and Countermeasures: https://www.cisecurity.org/blog/ransomware-facts-threats-and-countermeasures/
- CIS Primer: https://www.cisecurity.org/white-papers/ms-isac-security-primer-ransomware/

© RWX Security Solutions

Trust, but Verify

- If it seems too good to be true…
- Trust your gut – Be a little skeptical
- When in doubt, ask - #1 way to defeat social engineering
- Procedures for transferring $
- Ask your vendors about their security
- Verify files & websites using Virus Total: virustotal.com

© RWX Security Solutions

Going for Help

- FBI Internet Crimes Complaint Center (IC3): https://www.ic3.**gov**/default.aspx
- DHS Cybersecurity and Infrastructure Security Agency (CISA)
- US-CERT Incident Reporting System: https://www.us-cert.gov/forms/report
- State Patrol and Local Police
- Your Bank & Insurance

© RWX Security Solutions

Resources

- SCORE Library: https://omaha.score.org/browse-library-63?f%5B0%5D=im_field_topics%3A71&f%5B1%5D=content%3Asecurity
- NIST Small Business Cybersecurity Corner: https://www.nist.gov/itl/smallbusinesscyber
- FTC: Cybersecurity for Small Business: https://www.ftc.gov/tips-advice/business-center/small-businesses/cybersecurity
- SBA: https://www.sba.gov/managing-business/cybersecurity
- StaySafeOnline (NCSA): http://staysafeonline.org/
- StopThinkConnect (DHS CISA): https://stopthinkconnect.org/

© RWX Security Solutions

Small Business Cybersec

https://www.nist.gov/itl/smallbusinesscyber

NIST

Search NIST

NIST MENU

Information Technology Laboratory

SMALL BUSINESS CYBERSECURITY CORNER

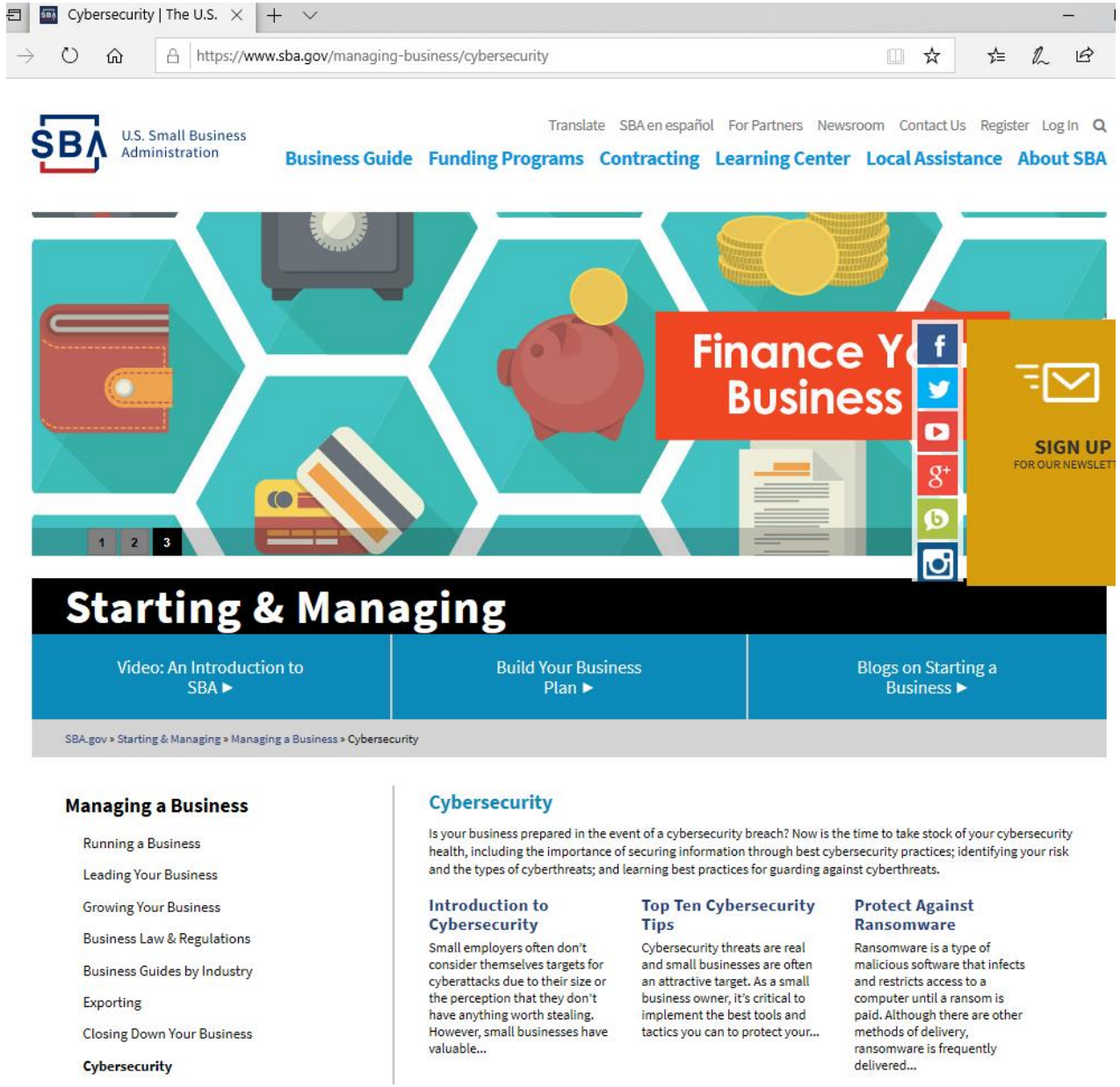
- Cybersecurity Basics +
- Planning Guides +
- Guidance by Topic +
- Responding to a Cyber Incident
- Training
- Contributor Directory
- FAQ
- Blog

CONNECT WITH US

Credit: Wendy Szwerc

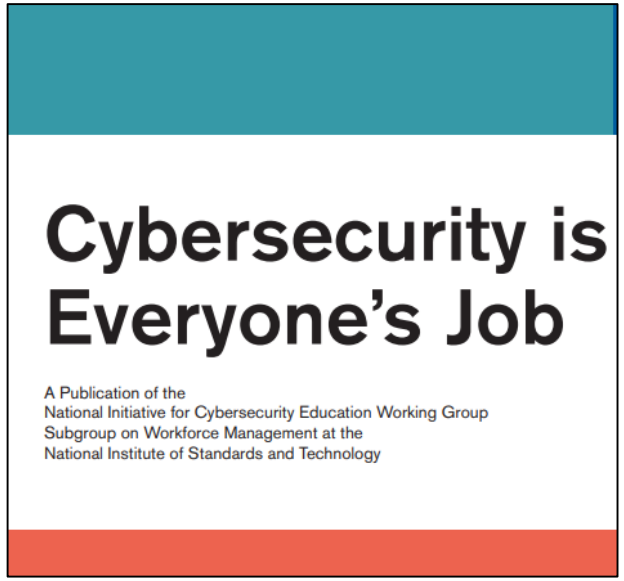
The vast majority of smaller businesses rely on information technology to run their businesses and to store, process, and transmit information. Protecting this information from unauthorized disclosure, modification, use, or deletion is essential for those companies and their customers.

https://www.ftc.gov/tips-advice/business-center/small-businesses/cybersecurity



https://www.sba.gov/managing-business/cybersecurity

http://www.dhs.gov/stopthinkconnect



https://www.nist.gov/sites/default/files/documents/2018/10/15/cybersecurity_is_everyones_job_v1.0.pdf

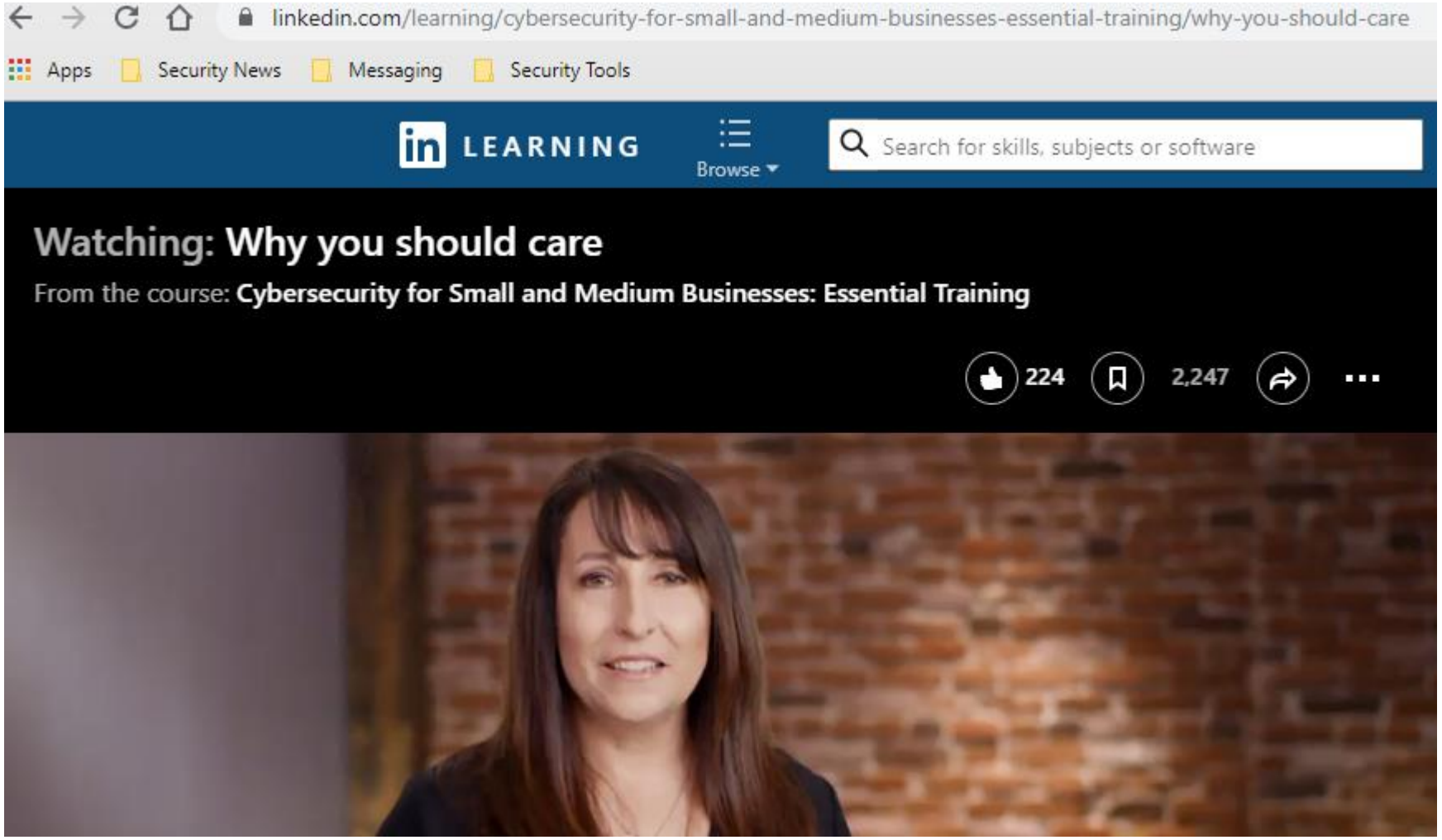
StaySafeOnline.org
National Cyber Security Alliance

http://staysafeonline.org/

INFRAGARD
MEMBERS ALLIANCE
IOWA

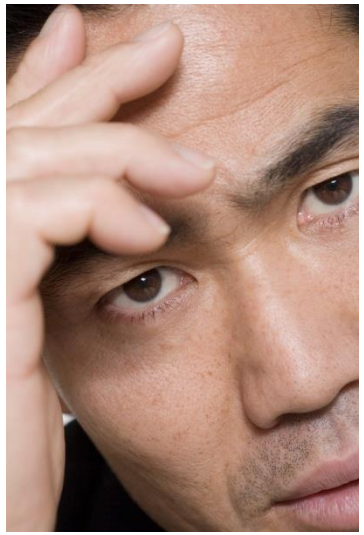
https://www.infragardiowa.org/

LinkedIn Learning



https://www.linkedin.com/learning/cybersecurity-for-small-and-medium-businesses-essential-training/

Who owns the Headache?



© RWX Security Solutions

Questions???

Ron Woerner, CISSP, CISM

Ron. Woerner @ rwxsecurity.com

Rwoerner @ Bellevue.edu

LinkedIn:

https://www.linkedin.com/in/ronwoerner/

Twitter: @ronw123

Share & Learn

Ron Woerner, RWX Security Solutions

CC BY NC SA