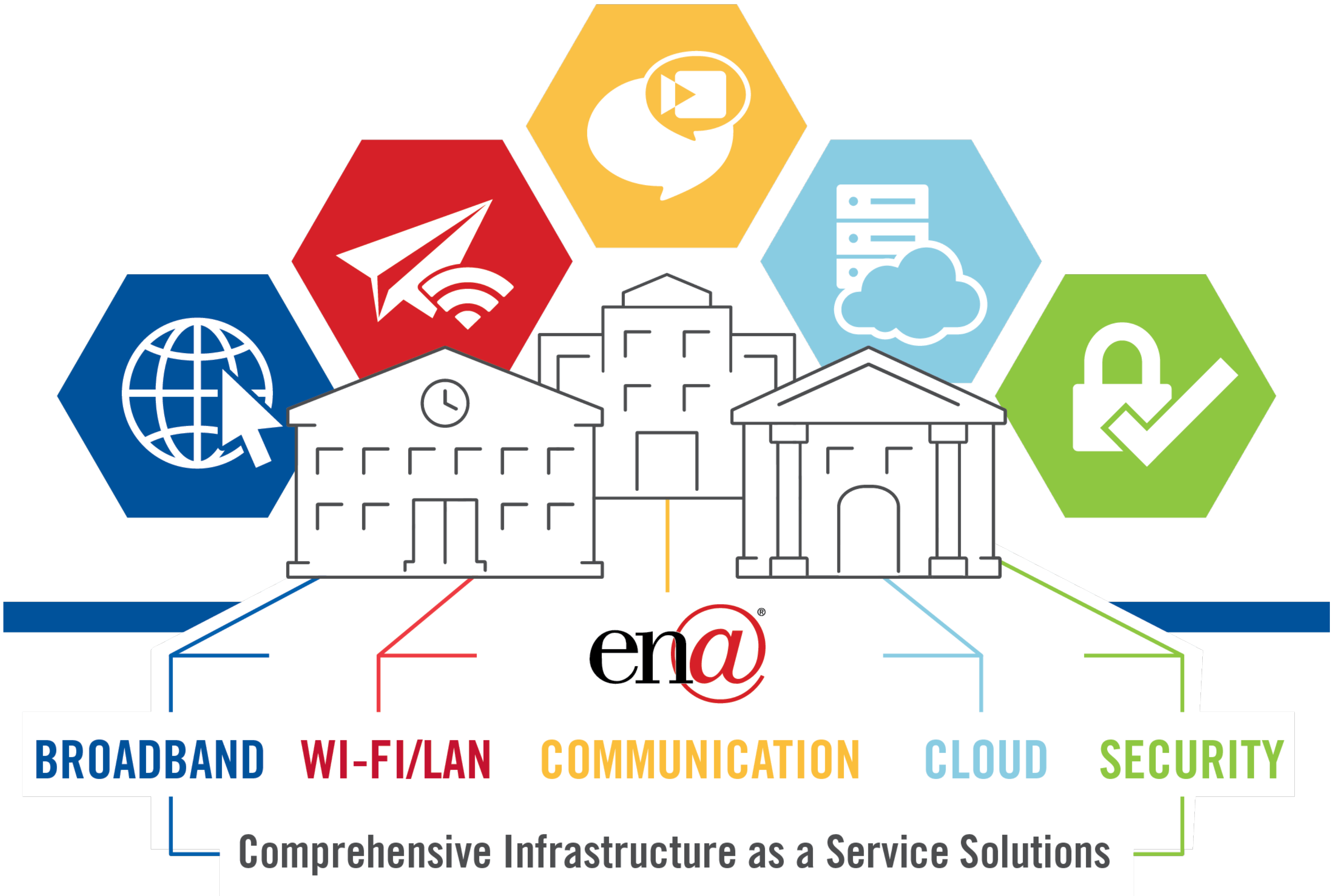
ena Education Networks of America®

Steps to Stay Safe from Cyber Threats

April 2022

Brian Hubbard

Connecting Communities Since 1996



BROADBAND WI-FI/LAN COMMUNICATION CLOUD SECURITY

Comprehensive Infrastructure as a Service Solutions

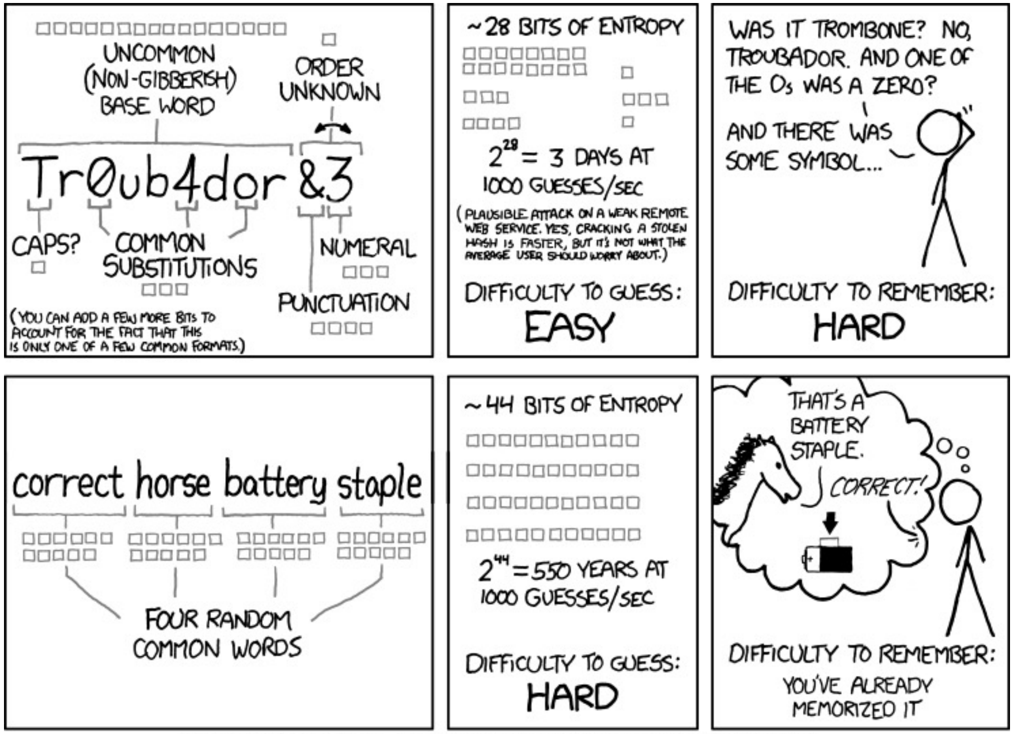
Biggest Security Issue We *See* Daily

Passwords and Authentication

I SHALL USE STRONG P@$$WORDS.
I SHALL USE STRONG P@$$WORDS.
I SHALL USE STRONG P@$$WORDS.
I SHALL USE STRONG P@$$WORDS.
I SHALL USE STRONG P@$$WORDS.

- Most password rules follow an old ideology, and they're hard to remember
- Resetting passwords takes up more time than anyone wants to admit
- Passwords are being shared

Passwords and Authentication


UNCOMMON (NON-GIBBERISH) BASE WORD
ORDER UNKNOWN
Tr0ub4dor &3
CAPS?
COMMON SUBSTITUTIONS
NUMERAL
PUNCTUATION
(YOU CAN ADD A FEW MORE BITS TO ACCOUNT FOR THE FACT THAT THIS IS ONLY ONE OF A FEW COMMON FORMATS.)
~28 BITS OF ENTROPY
2^28 = 3 DAYS AT 1000 GUESSES/SEC
(PLAUSIBLE ATTACK ON A WEAK REMOTE WEB SERVICE. YES, CRACKING A STOLEN HASH IS FASTER, BUT IT'S NOT WHAT THE AVERAGE USER SHOULD WORRY ABOUT.)
DIFFICULTY TO GUESS: EASY
WAS IT TROMBONE? NO, TROUBADOR. AND ONE OF THE Os WAS A ZERO?
AND THERE WAS SOME SYMBOL...
DIFFICULTY TO REMEMBER: HARD
correct horse battery staple
FOUR RANDOM COMMON WORDS
~44 BITS OF ENTROPY
2^44 = 550 YEARS AT 1000 GUESSES/SEC
DIFFICULTY TO GUESS: HARD
THAT'S A BATTERY STAPLE.
CORRECT!
DIFFICULTY TO REMEMBER: YOU'VE ALREADY MEMORIZED IT

THROUGH 20 YEARS OF EFFORT, WE'VE SUCCESSFULLY TRAINED EVERYONE TO USE PASSWORDS THAT ARE HARD FOR HUMANS TO REMEMBER, BUT EASY FOR COMPUTERS TO GUESS.

- New NIST Standards:
  - The more characters the better
  - No more password change cycles
  - Passphrases – not complicated passwords
- Problem: Vendors may not adopt this quickly, so you'll be at their mercy for many of your applications
- Change all default passwords
- Multi-Factor Authentication!!!
- Future – fewer passwords, more biometrics

Phishing

- Accounts for 96% of all socially-based security attacks
- COVID-19 related phishing attacks started even before high case numbers in March 2020 in USA
- Avg. financial loss to compromised institution is over $50,000/account
- Avg. additional loss by individuals targeted by identity theft is $5,000
- Phishing attempts often appear to come from persons in authority
- Senior employees are often the most vulnerable

Phishing

- User training: Leverage phishing simulations that make the training relate to the user's personal life – what would hurt most?
- Avoid links/emails/comments with lots of typos, poor English.
- Make sure that links go to where they say they go. A link for American Express should not go to hady.teixeira@tjam.jus.br
- Set rules: An example might be, "You will never receive an email asking for W2 information."
  - If someone does get it, they can say no, or they should go find the sender *in person* to confirm
- Try to use an email service with strong technology to block spam and phishing

Internet of Things

- Understand the security issues that could arise with these new devices.
- Review the policies and security protocols of vendors before buying that new gadget:
  - Have they been penetration tested?
  - What data are they collecting and where and why are they keeping it?
- Change all default passwords. Always
- Get a password manager

Ransomware / Malware

- Global ransomware damage costs were $29 MILLION in 2020 – more than 200x increase over 2019
- The number of ransomware attacks rose 158% from 2019 to 2020
- The most effective protection against ransomware is **backup and disaster recovery**, followed by training
- Ransomware and Malware is often installed but sitting dormant for 6 months or more before activating. You may feel safe, but you may already be infected.

Ransomware / Malware

- Create and update a response plan every year; make sure cross-functional teams are involved
- Implement a Unified Threat Management tool or other solution to continuously check for malware
- Have a backup strategy and test those backups at least once per year
- Be suspicious of both the “too good to be true” and the “wow, what a coincidence” situations.
- Apple/Microsoft/Google DO NOT put a phone number on your device to call for technical support/virus removal, et cetera.

Phone Scams

Telephone scams continue to increase and continue to be harder to identify.

- 65% of Americans have lost money to a phone scam in the past year (20% of those, more than once)
- On average, each scam victim lost $502, totaling about $29.8 billion overall.
- The IRS will not call you (unless you've ignored letters and owe a lot)

Phone Scams

- Neighbor Spoofing on the rise
- Let unknown ## go to voicemail
- Don’t call a missed number back
- Hang up. Some scams record your answers to simple questions to build audio of YOU saying you want to buy something, like a timeshare.
- Report scams immediately to the FTC and local authorities

Hidden Vulnerabilities

- Hackers are scanning your network for vulnerabilities – but are you?
- Without good understanding of what's on your network, it is almost impossible to focus and prioritize work
- Attackers and malicious code linger undetected in breached networks for an average of 191 days
- Your environment changes constantly, regular checks are critical

Data Privacy

BANK • PASSPORT NUMBER • SCHOOL • JOB • COLLEGE • BANK ACCOUNT • CITY OF BIRTH • ADDRESS • CITIZENSHIP • GENDER • DISABILITY • DATE OF BIRTH • GED • RACE • TELEPHONE NUMBER • EMAIL • ARREST • SALARY • DRIVER'S LICENSE • AGE • SOCIAL SECURITY NUMBER • DIPLOMA

A child's identity is worth more on the dark web and is over 50% more likely to be compromised than an adult's.

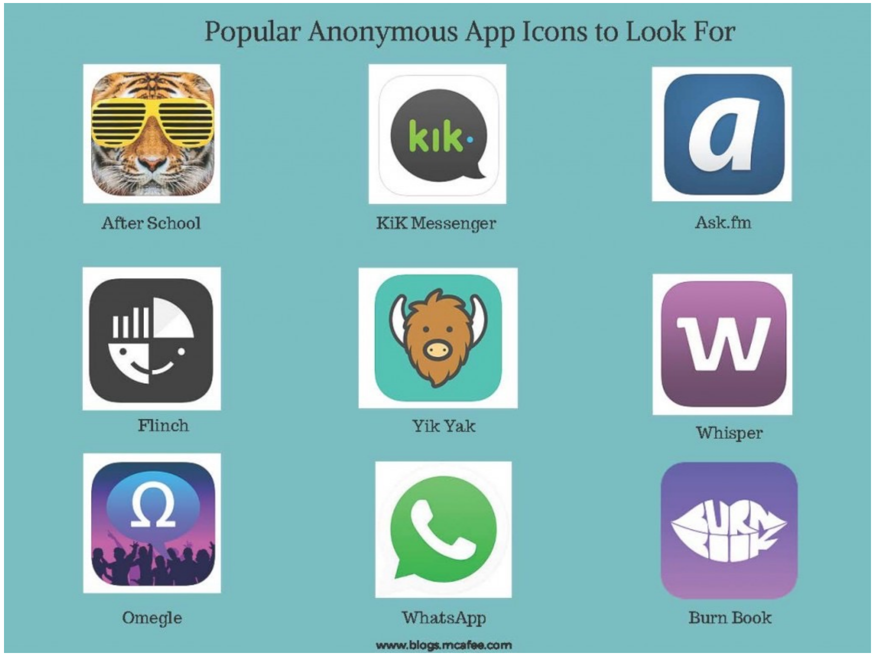
- It's hard to protect what you can't see
- New applications are being introduced without library's knowledge or verification of security practices and policy compliance
- Tracking 3rd party access and policies is a big challenge
- Compliance to state requirements is a growing challenge without the tools and processes needed
- You have valuable data, are you tracking who has access to it and when they are accessing it? How does access to that data impact digital and physical safety?

Threats Facing Children and Teens in 2022

“Although it may seem that malware attacks and cybercrime live in the adult world, cyber thieves regularly target children and teens where they’re most active – chat rooms, social media, video streaming sites and online video games. Children are good targets because they may have high levels of trust in people and low levels of knowledge in cybersecurity.”

StaySafeOnline.org

Anonymous Sharing



- Not all anonymous apps are bad; After School does include resources for counseling and other items. Be careful and understand risks.
- Still too many teens that believe what they post has no impact on their future. Share examples: Disney fired James Gunn from Guardians of the Galaxy Vol. 3 for social media posts from over ten years ago.
- Our digital reputations are very difficult to change or remove. Protect your reputation as much as your identity.

Digital Purchases and Piracy

- Teach teens about good sites to purchase from, and what to look for in sites you have never heard of. Always look for security lock in browser. Research the site. Use Private Browsing mode in web browser so site won't keep tracking you and sending you ads
- Stealing is stealing. And teens DO GET CAUGHT. ENA receives Digital Millennium Copyright Act take down notices almost every day for violations in schools and libraries. Remember digital reputation? This puts people in jail.

Sexting

- Say no. Yes, this is hard to do, and it may cause you to lose a relationship. Hopefully, you will be able to look back at that in the future and say GOOD.
- REPORT IT. Especially if someone sends you explicit material or attempts to take advantage of you. REPORT IT to your school, police, National Center for Missing and Exploited Children, and others. You may be saving a life.
- Take a look at "A Teens Guide to Cyber Security" for more info about sexting and the consequences (did we mention jail?) https://www.hotspotshield.com/resources/teens-guide-to-cyber-security/

Additional Vulnerabilities

- Understand that once a “friend” is on your home Wi-Fi, they could use an anonymous email site to send a death threat to the president and the IP address will lead to your house.
- Change the default passwords on your network gear. I can login to my neighbor’s Wi-Fi access point even after telling him YEARS AGO.
- Think 10 times about why you really need your friend to be able to login to Snapchat and post for you to keep your streak going. Is it really worth it? Or Twitter, or Instagram, or…

More Resources

- https://blog.techsoup.org/posts/cybersecurity-checklist-for-when-your-library-reopens
- https://blogs.ifla.org/lpa/2020/03/27/awareness-planning-resilience-thoughts-on-libraries-cyber-defense-in-2020/
- https://www.railslibraries.info/system/files/Anyone/mtg/135822/IT%20Security%20Part%201%20slides.pdf

Questions