Preparing for the Unexpected

Mitigate and Eliminate Cybersecurity Threats
Welcome

Simon Weller
Director of Technology
Successfully Serving

6,000 + Sites Across America!

ONE out of every 14 public school students and staff are served by ENA solutions

E-rate Top 5 Service Provider

More than $755 Million in E-rate Funding Approvals

550+ School Districts

320+ Library Systems

3.5m+ Students and Staff

4.5m+ Library Patrons
Exceptional Performance

CUSTOMER RETENTION since 2007 has been greater than 97% of surveyed customers said they would RECOMMEND ENA TO OTHERS.

Our overall customer satisfaction rating is 99%.

24x7x365 CUSTOMER SUPPORT 99% Proactive Support Less than 40 sec average wait time 94% First Contact Solutions

Delivering Services in 34 States
ENA Points of Presence
Connections to Internet
Comprehensive Infrastructure as a Service Solutions for K–12 Schools, Higher Education Institutions, and Libraries
Current Security Landscape
"Think we can say we didn't see it coming?"
Current Security Landscape

- Phishing and Ransomware attacks
  - According to Social Engineer Research, phishing accounts for 77% of all socially based attacks
  - Business targeted lose $43,000 per account
  - Individuals targeted through impersonation lost $4,200 on average
  - Often appear to come from persons with authority
  - Your senior employees are often the most vulnerable
Current Security Landscape

• Ransomware on the rise!
  - Encrypts your data and demands money to get your files back
  - EternalBlue (WannaCry et al) exploited a previously patched Windows flaw in the SMB (file sharing) protocol
  - 200K victims and 300K infected computers in over 150 countries
  - Microsoft released an emergency patch for XP and Server 2003
  - Was halted by registering a “kill switch” domain.
  - A network at Boeing was affected on March 28th of this year!
Current Security Landscape

• Meltdown and Spectre
  – Exploits CPU features to gain access to data
  – All major Operating Systems are patched for Meltdown and Spectre V1
  – Spectre V2 requires Intel Microcode (Linux can use Reptoline)
  – Local Privilege Escalation
  – Spectre can be exploited via javascript – new browser releases try to isolate memory between threads to prevent this
  – Almost EVERYONE caught of guard
"I don't know about 'advanced', but he certainly is a persistent threat!"
How bad is DDoS?
Last days, we got lot of huge DDoS. Here, the list of "bigger that 100Gbps" only. You can see the simultaneous DDoS are close to 1Tbps!

- 1 Tbps
- 150,000 compromised IOT devices
DDOS Landscape

- Getting bigger and bigger
  - 1.2Tb/s against github.com
  - ... 5 days later - 1.7Tb/s against a well known US service provider
  - Not just enterprise or for profit targets
  - Numerous 30-60Gb/s attacks against K-12 in the last 6 months
  - Unsecured Memcached is the new vector of choice
  - Common methods include unsecured DNS servers, NTP servers
Kansas adds defensive barrier after cyberattack shuts down student testing

The attacks, known as a “distributed denial of service,” began March 27, with some overseas sites bombarding the computer server with intense volumes of data. A new assault Tuesday from both domestic and international locations crashed the system.

California students hit by DDoS attack, unable to take tests

On May 1, Oakland Unified School District in California was potentially hit by a distributed denial-of-service attack that left hundreds of thousands of students unable to log in to take their Common Core assessments, according to CBS. This event occurred to the dismay of educators and students alike, who had spent weeks preparing to take the mandatory tests only to be denied access.

“Not just the days of the test that are affected,” said Johanna Parasio, Common Core Testing Coordinator for Fremont High. “It’s not a test day. It’s a whole week of testing.”

Two Idaho students face charges after DDoS attacks against school district

A 17-year-old Idaho high-schooler and a middle school student could face felony charges for a series of distributed denial of service (DDoS) attacks against the West Ada School District in Mendon last week.
How easy is it?
How easy is it?

Free Trial!
All members can enjoy up to 200 Mbps for 300 seconds... for free!

Try For Free Today!

* No credit card required, subject to terms of use and network availability

Gabriel Gonzalez (xStrikerBoss) 4 days ago
+Vulpus you could use ipstresser.com
u can get a free trial then u make another account and do the same lol

Reply ⋅ 👍 ⋅ ⌒
Emerging Threats
Cloud Computing

- Software as a Service (SaaS)
  - How safe is your data?
  - Make sure you know how your data is being handled
  - Is it being backed up?
- Infrastructure as a Service (IaaS)
  - Does your vendor support encryption?
  - Who owns the keys?
  - Do they offer a private environment?
Evolving Standards
"How long do you think it will take to crack the password?"
Passwords

• Passwords aren’t very secure
  – Painful for most of remember
  – So people create variations...
  – ...or write them down...
  – ...or use the same password everywhere
  – We force password changes for no reason
NIST Standards

- National Institute of Standards and Technology
  - Intended for Federal Gov applications, but used by many as a benchmark
  - New SP 800-63 covers Registration/Authentication/Assertions
  - Strong user experience emphasis. Make your passwords user friendly so users don’t cheat!
  - Place burdens on the verifier, not the users
  - Don’t ask the user to do things that don’t significantly improve security
  - 8 character minimum, max of at least 64 characters (inc emojis!)
Passwords aren’t very secure

- Dual/multi factor authentication needed
- Password policies are involving

**Tr0ub4dor & 3**

Uncommon (non-gibberish) base word

Order unknown

Caps? Common substitutions

Numerals

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 vs. cracking a strong hash is faster, but it’s not what the average user should worry about.)

Difficulty to guess: **EASY**

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**

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.
NIST Standards

• New password standards
  - Longer
  - Less complex and easier to remember
  - Allows for spaces
  - Should include blacklisted words/phrases to reduce bad choices
  - Dual factor support
17-factor authentication
Protect your data

- Mobile Assets
  - Use disk encryption
  - Use remote utilities that can disable a stolen device

- Use one account per user
  - Never share credentials
  - Provides logs on a per user basis
  - User Dual/Multi factor authentication where possible
Protect your Network

- Wifi
  - Use 802.1x authentication to tie users to your directory service
  - If providing guest access, separate them from your internal users
  - Secure the hardware
  - Tune the signal to the area the AP needs to cover
  - Rogue AP detection
  - Mobile Device Management (MDM) for control
Protect your Network

• Switch ports
  - Controlled access (802.1x/captive portal/mac auth bypass)
  - ...or port security if that’s your only option
  - Loop management or disable unused ports
  - Separate Admin, Teachers and Students using VLANs (access technology can do this for you, e.g. VLAN steering or acl enforcement based on user group policy)
  - Macsec (802.1ae) supports L2 encryption between machines/VMs and is also supported by newer switches
Acceptable Use Policies

- Make sure you have an AUP
  - Make sure your faculty and students receive and agree to it
  - Clearly state the penalties of violations
  - Make sure it covers all school owned assets
  - If you allow BYOD, those users also need to be covered by your AUP
Educate Your Internal Customers

- Education is the **number one** defense!
  - Hold sessions on how to spot a phishing email or call
  - Get your Superintendent on board so all senior staff are trained – as they are the most vulnerable!
  - Take out the culture of fear and make sure everyone is transparent and honest so you can shut down a compromise quickly
  - Make sure you teachers NEVER share any access credentials
  - If a common phishing attack is on the loose, inform your users on how to spot it
Free Phishing Testing – getgophish.com

Set Templates & Targets
Gophish makes it easy to create or import pixel-perfect phishing templates.

Our web UI includes a full HTML editor, making it easy to customize your templates right in your browser.

Launch the Campaign
Launch the campaign and phishing emails are sent in the background. You can also schedule campaigns to launch whenever you'd like.

Track Results
Detailed results are delivered in near real-time. Results can be exported for use in reports.
What if you are compromised?

- Have a backup plan
  - Consider Insurance cover for compromises
  - Every organization should have a Disaster Recovery Plan
  - Make sure you assess the risk to each part of your organization
  - Determine what is most important and document a recovery order
  - Set clear recovery objectives
  - Find a trusted partner that can help you build a plan if needed
QUESTIONS?

Contact ENA Today

www.ena.com
@ENAconnects facebook.com/ENAconnects