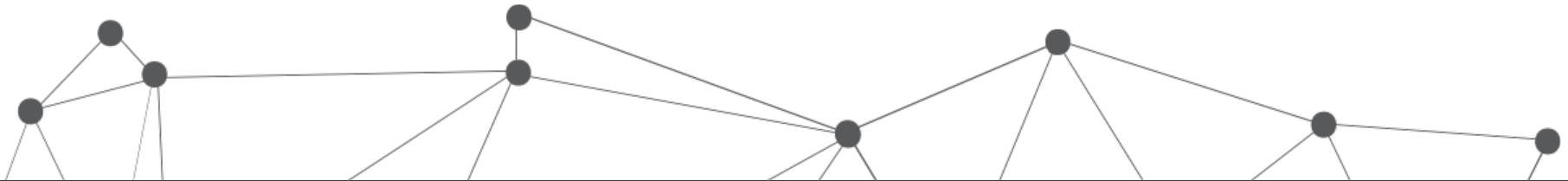


Preparing for the Unexpected

Mitigate and Eliminate Cybersecurity Threats

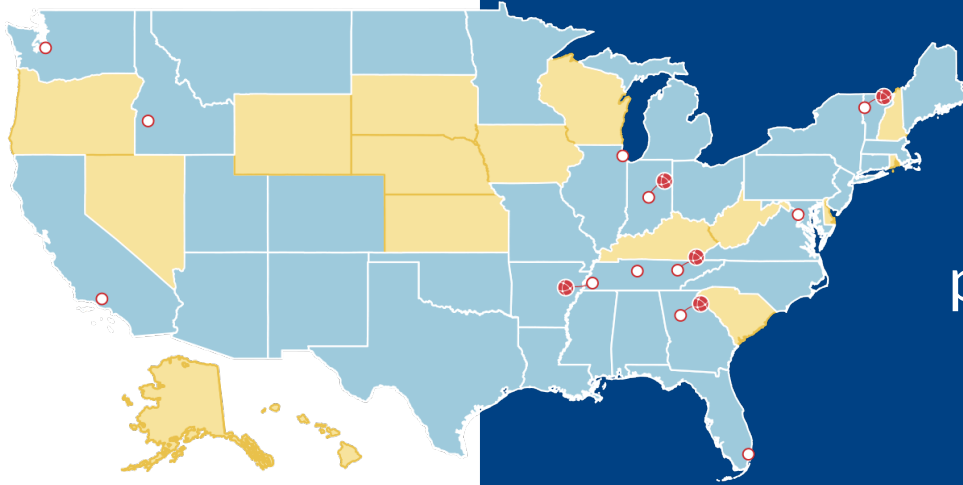
Welcome

Simon Weller
Director of Technology





Connections to INTERNET[®] 2



More than
\$755 Million
in E-rate Funding
Approvals

6,000 + Sites Across America!

public school students and staff
are served by ENA solutions

School Districts

Library Systems

Students and Staff

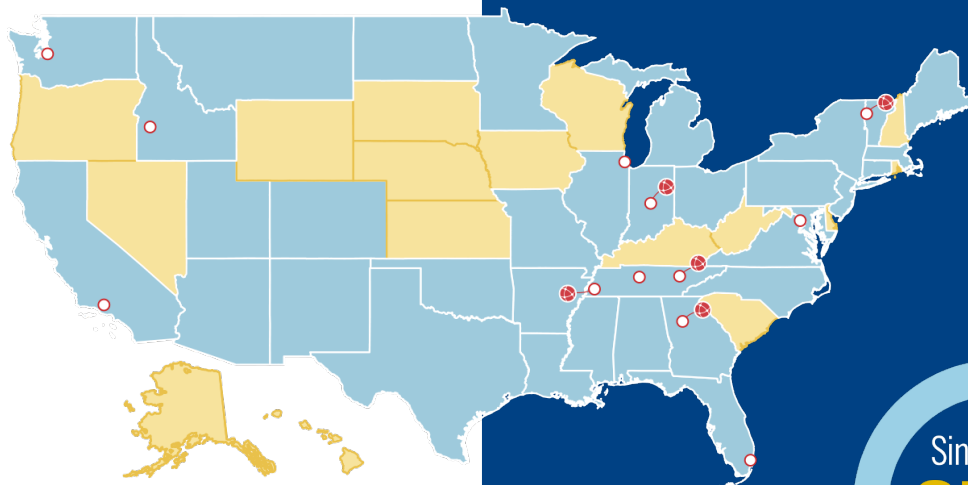
Library Patrons

Exceptional Performance

Delivering Services in **34** States

EN A Points of Presence

Connections to **INTERNET**



Our overall customer satisfaction rating is

99%

24x7x365
CUSTOMER SUPPORT

99%
Proactive Support

Less than
40sec
average wait time

94%
First Contact Solutions

**CUSTOMER
RETENTION**

since 2007 has
been greater than

97%

of surveyed customers
said they would

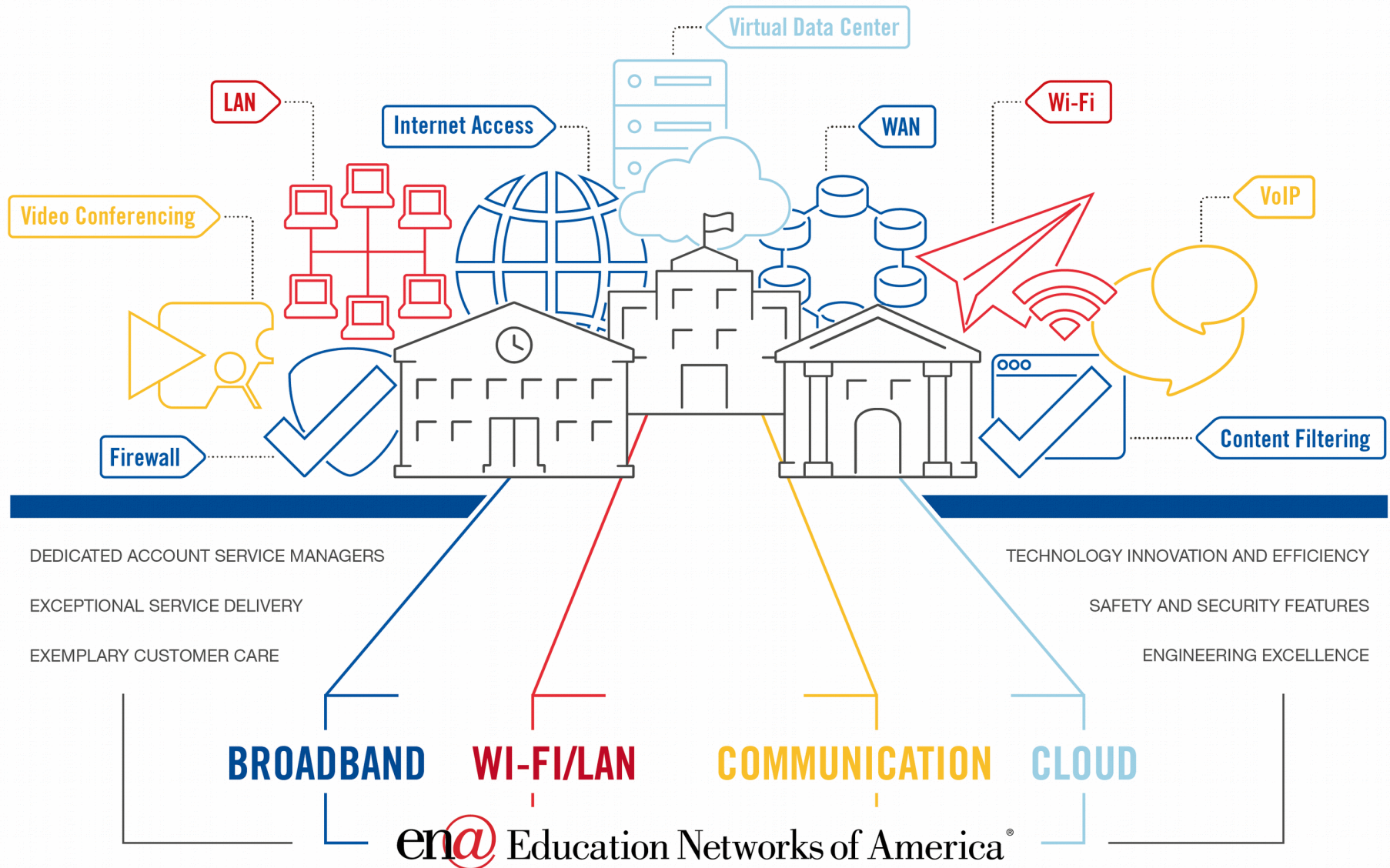
**RECOMMEND
ENA TO OTHERS**

Since 2007

97%

Comprehensive Infrastructure as a Service Solutions

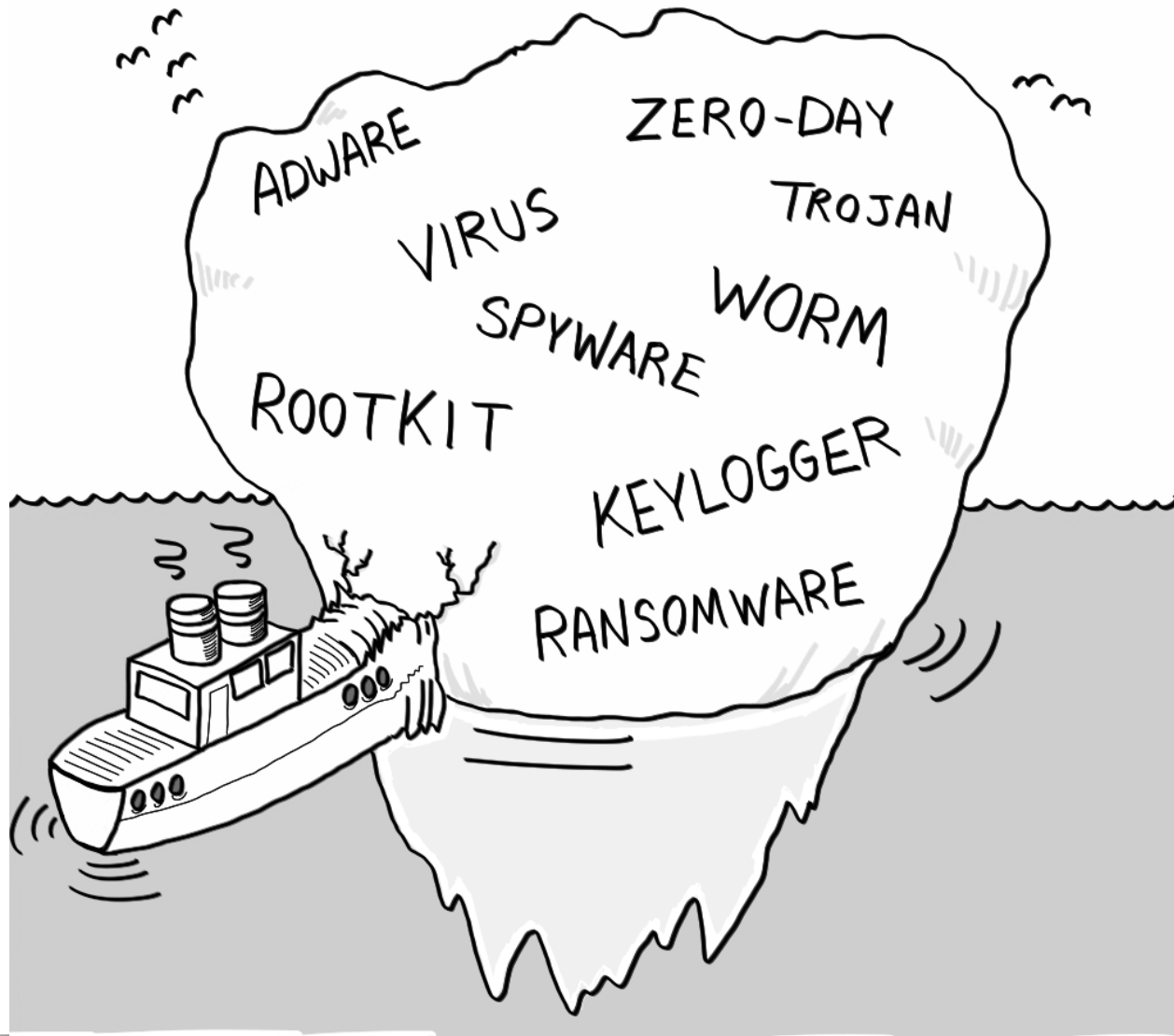
for K-12 Schools, Higher Education Institutions, and Libraries





Current Security Landscape

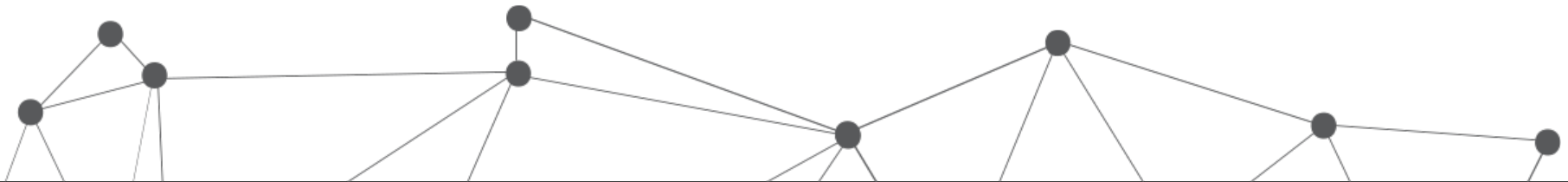




"Think we can say we didn't see it coming?"

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

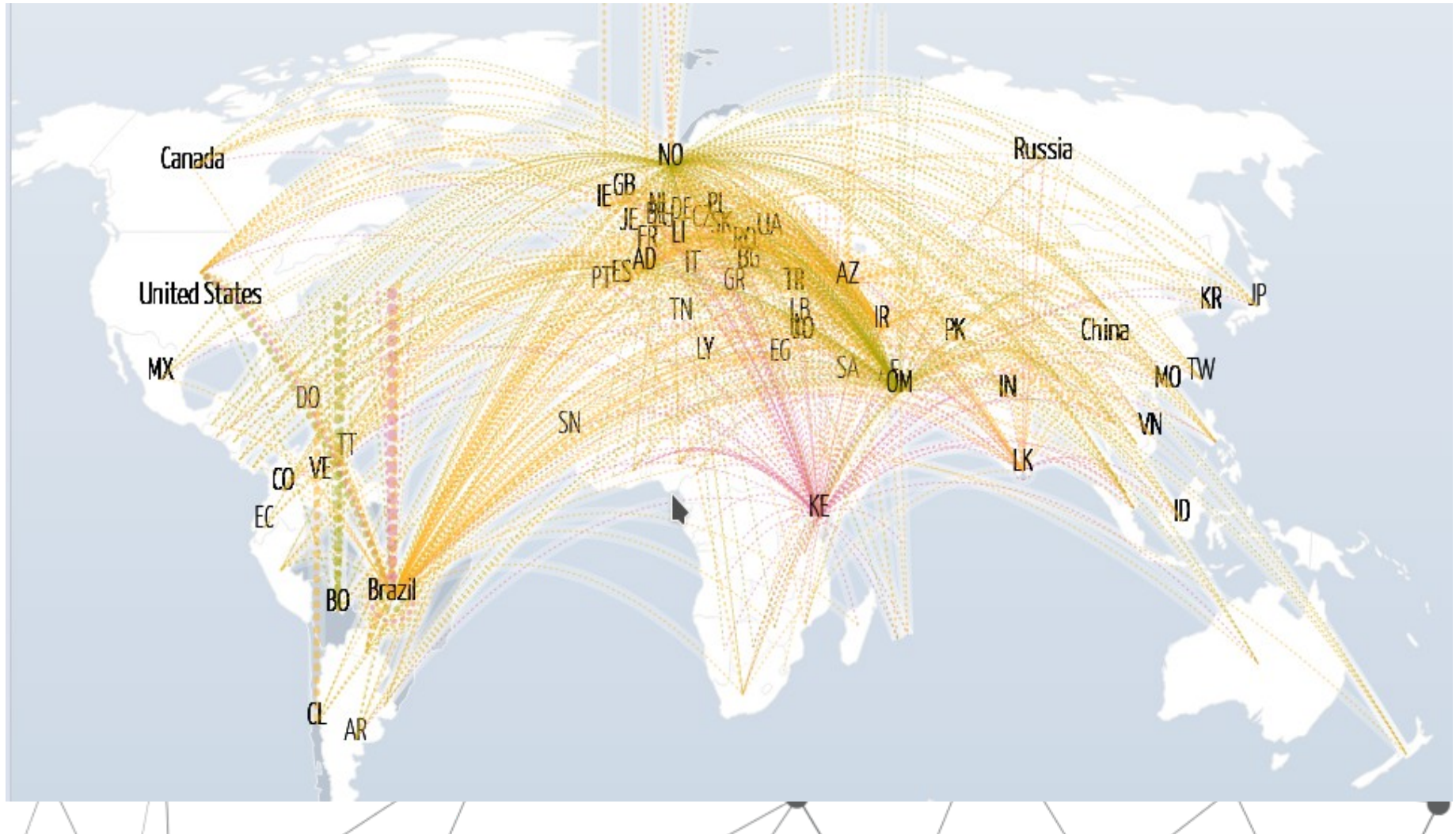


DESIGNERHIPSTER.COM



"I don't know about 'advanced', but he certainly is a persistent threat!"

How bad is DDoS?





Octave Klaba / Oles

@olesovhcom

Follow



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

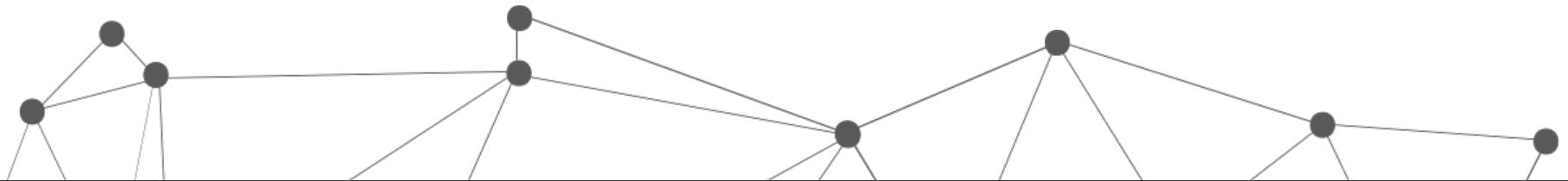
```
log /home/vac/logs/vac.log-last | egrep "pps\|.....  
bps" | awk '{print $1,$2,$3,$6}' | sed "s/ /|/g" | cut -f  
1,2,3,7,8,10,11 -d '|' | sed "s/.....bps/Gbps/" | sed  
"s/.....pps/Mpps/" | cut -f 2,3,4,5,6,7 -d ":" | sort | g  
rep "gone" | sed "s/gone|/"  
Sep|18|10:49:12|tcp_ack|20Mpps|232Gbps  
Sep|18|10:58:32|tcp_ack|15Mpps|173Gbps  
Sep|18|11:17:02|tcp_ack|19Mpps|224Gbps  
Sep|18|11:44:17|tcp_ack|19Mpps|227Gbps  
Sep|18|19:05:47|tcp_ack|66Mpps|735Gbps  
Sep|18|20:49:27|tcp_ack|81Mpps|360Gbps  
Sep|18|22:43:32|tcp_ack|11Mpps|136Gbps  
Sep|18|22:44:17|tcp_ack|38Mpps|442Gbps  
Sep|19|10:13:57|tcp_ack|10Mpps|117Gbps  
Sep|19|11:53:57|tcp_ack|13Mpps|159Gbps  
Sep|19|11:54:42|tcp_ack|52Mpps|607Gbps  
Sep|19|22:51:57|tcp_ack|10Mpps|115Gbps  
Sep|20|01:40:02|tcp_ack|22Mpps|191Gbps  
Sep|20|01:40:47|tcp_ack|93Mpps|799Gbps  
Sep|20|01:50:07|tcp_ack|14Mpps|124Gbps  
Sep|20|01:50:32|tcp_ack|72Mpps|615Gbps  
Sep|20|03:12:12|tcp_ack|49Mpps|419Gbps  
Sep|20|11:57:07|tcp_ack|15Mpps|178Gbps  
Sep|20|11:58:02|tcp_ack|60Mpps|698Gbps  
Sep|20|12:31:12|tcp_ack|17Mpps|201Gbps  
Sep|20|12:32:22|tcp_ack|50Mpps|587Gbps  
Sep|20|12:47:02|tcp_ack|18Mpps|210Gbps  
Sep|20|12:48:17|tcp_ack|49Mpps|572Gbps  
Sep|21|05:09:42|tcp_ack|32Mpps|144Gbps  
Sep|21|20:21:37|tcp_ack|22Mpps|122Gbps  
Sep|22|00:50:57|tcp_ack|16Mpps|191Gbps  
You have new mail in /var/mail/root
```

10:37 PM - 21 Sep 2016



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



Alert 53° Sign In | Subscribe

THE KANSAS CITY STAR.

10 WEEKS FOR \$10
TRUE BLUE STAR SUBSCRIBE NOW!

NEWS SPORTS BUSINESS FOOD

UMKC | Executive MBA
Henry W. Bloch School of Management
UNIVERSITY OF MISSOURI-KANSAS CITY

LEAD WITH CONFIDENCE.

Local APRIL 2, 2014

Kansas adds defensive barrier after cyberattack shuts down student testing

HIGHLIGHTS
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.

FireBreak
ARCTICWOLF

services resources about contact

California students hit by DDoS attack, unable to take tests

 Tom Clare
May 6th, 2015

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.



"It's not just the days of the test [that are affected]," said Johanna Paraiso, Common Core Testing Coordinator for Fremont High. "It's

SC MAGAZINE
FOR IT SECURITY PROFESSIONALS

> SC US
SC UK

Fake bitly links used to distribute malware, spam

Federal R of STL re password DNS att

NEWS PRODUCTS BLOGS RESOURCES VIDEOS WHITEPAPERS

SC Magazine > News > Two Idaho students face charges after DDoS attacks against school district

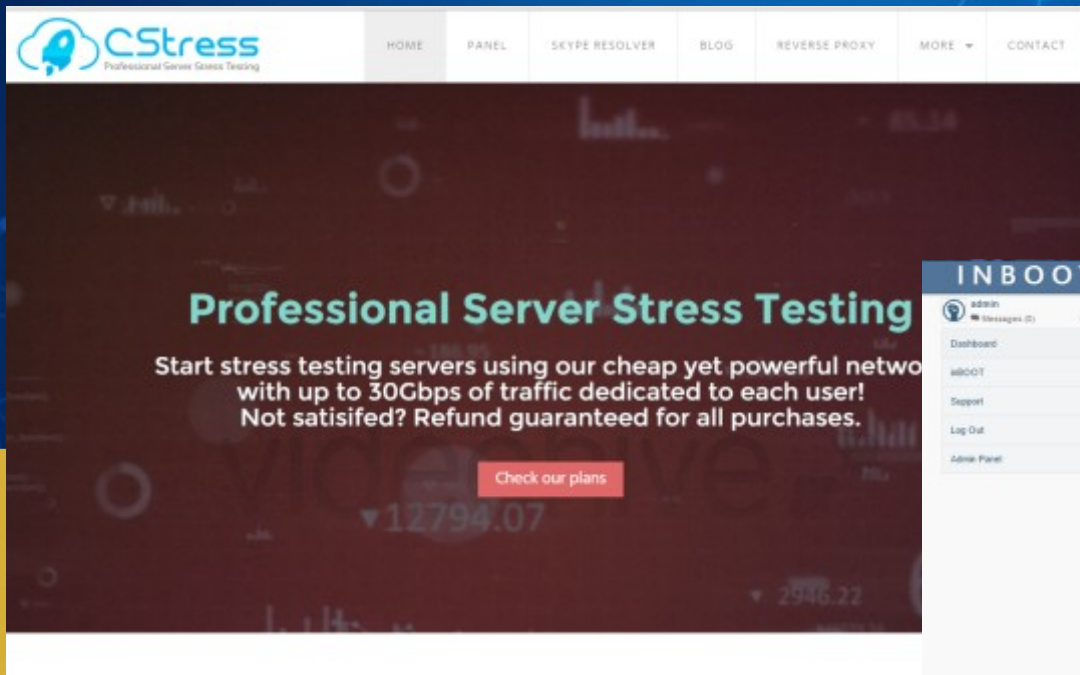
Robert Abel, Content Coordinator
May 18, 2015

Two Idaho students face charges after DDoS attacks against school district

Share this article:       

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 Meridian last week.

How easy is it?



The image shows the homepage of the CSstress website. The header features the CSstress logo and navigation links: HOME, PANEL, SKYPE RESOLVER, BLOG, REVERSE PROXY, MORE, and CONTACT. The main content area has a dark background with the text "Professional Server Stress Testing" in large green letters. Below this, it says "Start stress testing servers using our cheap yet powerful network with up to 30Gbps of traffic dedicated to each user! Not satisfied? Refund guaranteed for all purchases." A red button labeled "Check our plans" is positioned below the text. The background of the website features faint, glowing network diagrams.

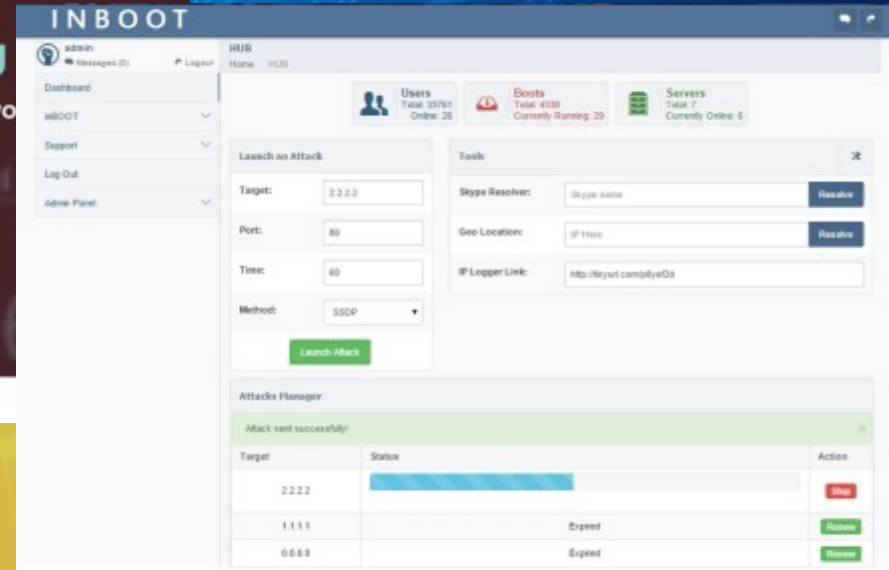
CSstress
Professional Server Stress Testing

HOME PANEL SKYPE RESOLVER BLOG REVERSE PROXY MORE CONTACT

Professional Server Stress Testing

Start stress testing servers using our cheap yet powerful network with up to 30Gbps of traffic dedicated to each user!
Not satisfied? Refund guaranteed for all purchases.

[Check our plans](#)



The image shows the INBOOT dashboard interface. The top bar includes the INBOOT logo, user information (admin, Messages (2), Logout), and navigation links (Home, HUB). The dashboard displays several statistics: Users (Total: 25, Online: 25), Boots (Total: 4338, Currently Running: 29), and Servers (Total: 7, Currently Online: 6). The main section is titled "Launch an Attack" and contains input fields for Target (2.2.2.2), Port (80), Time (60), and Method (SSCP). A "Launch Attack" button is present. To the right, there is a "Task" section with input fields for Skype Resolver, Geo Location, and IP Logger Link, each with a "Resolve" button. Below these sections is an "Attacks Manager" table showing a list of attacks with columns for Target, Status, and Action.

INBOOT

admin Messages (2) Logout Home HUB

Dashboard

- allCOT
- Support
- Log Out
- Admin Panel

Users
Total: 25
Online: 25

Boots
Total: 4338
Currently Running: 29

Servers
Total: 7
Currently Online: 6

Launch an Attack

Target:

Port:

Time:

Method:

[Launch Attack](#)

Task

Skype Resolver: [Resolve](#)

Geo Location: [Resolve](#)

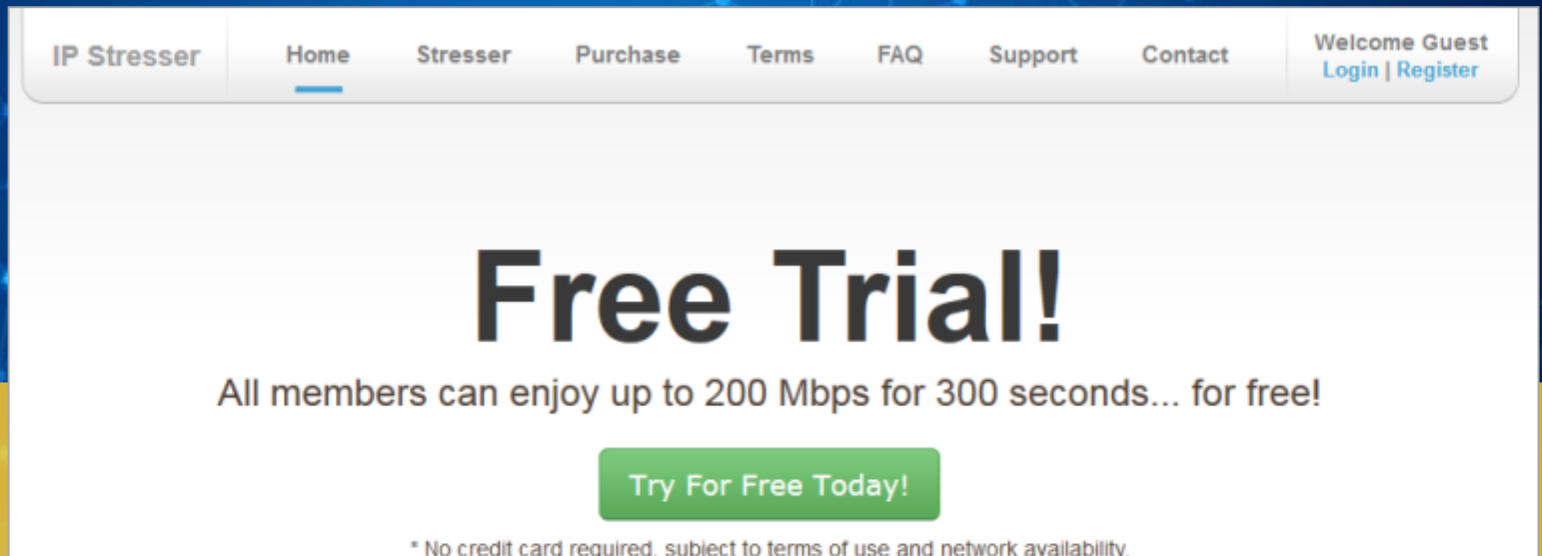
IP Logger Link:

Attacks Manager

Attack sent successfully!

Target	Status	Action
2.2.2.2	<div></div>	Stop
1.1.1.1	Expired	Remove
0.0.0.0	Expired	Remove

How easy is it?



The screenshot shows the homepage of a website called 'IP Stresser'. The navigation bar at the top includes links for 'IP Stresser', 'Home' (which is underlined), 'Stresser', 'Purchase', 'Terms', 'FAQ', 'Support', and 'Contact'. On the right side of the navigation bar, it says 'Welcome Guest' with links for 'Login' and 'Register'. The main content area features a large 'Free Trial!' heading, followed by the text 'All members can enjoy up to 200 Mbps for 300 seconds... for free!'. Below this is a green button that says 'Try For Free Today!'. At the bottom of the main content area, there is a small disclaimer: '* 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 ·  

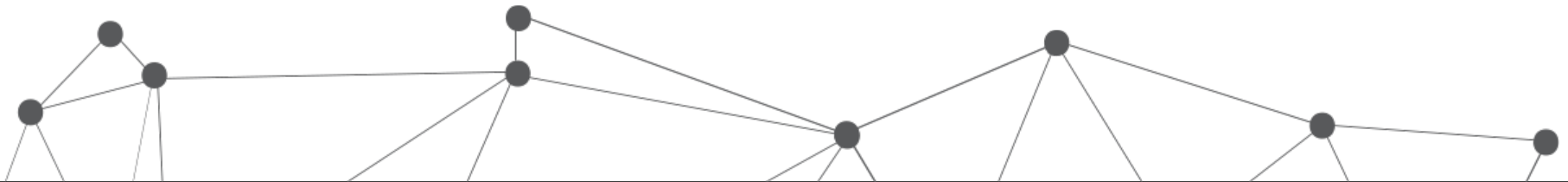


Emerging Threats



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

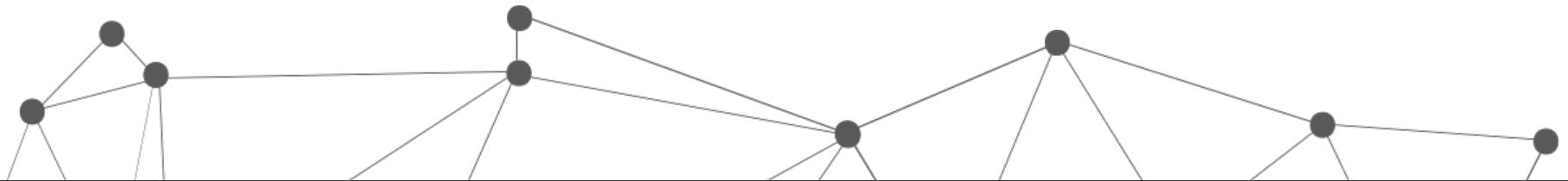




"How long do you think it will take to crack the password?"

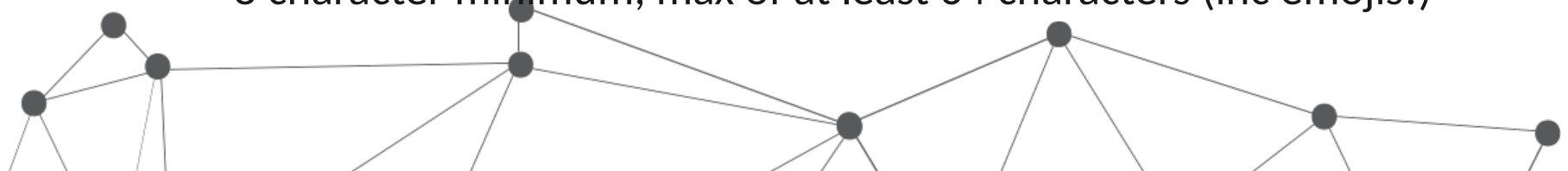
Passwords

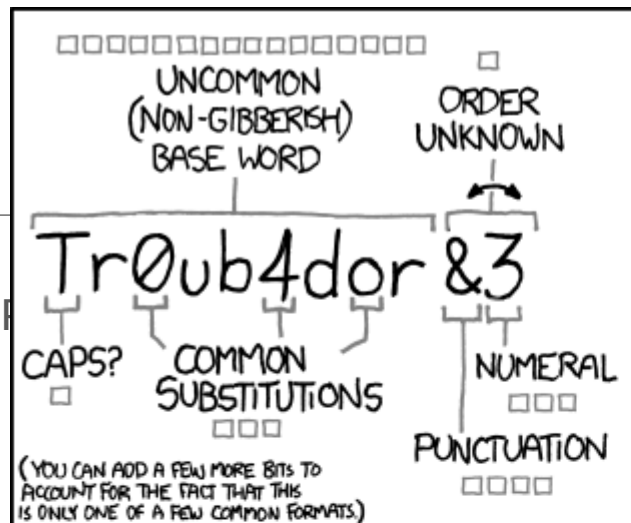
- Passwords aren't very secure
 - Painful for most of remember
 - So people create variations...
 - ...or write them down...
 - ...or use the same password everywhere
 - We force password changes for no reason



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!)





~28 BITS OF ENTROPY

□□□□□□□□ □
 □□□□□□□□ □□□
 □□□□ □

$2^{28} = 3 \text{ DAYS AT } 1000 \text{ GUESSES/SEC}$

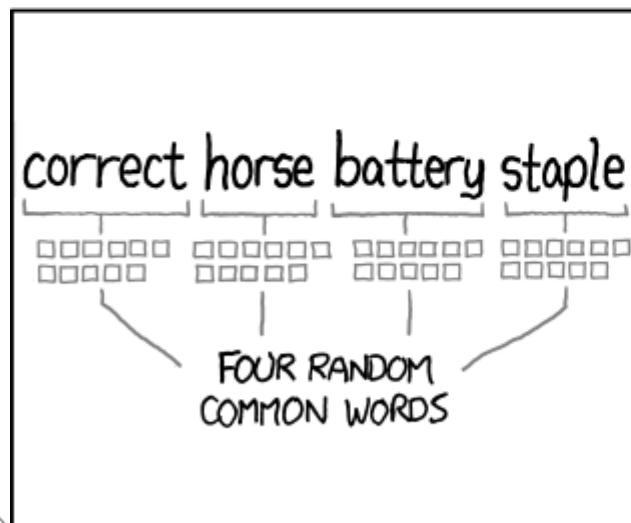
(PLAUSIBLE ATTACK ON A WEAK REMOTE WEB SERVICE: YES, CRACKING A STOLEN HASH IS FASTER, BUT IT'S NOT WHAT THE AVERAGE USER SHOULD WORRY ABOUT.)

DIFFICULTY TO GUESS: **EASY**

WAS IT TROMBONE? NO, TROUBADOR. AND ONE OF THE 0s WAS A ZERO?

AND THERE WAS SOME SYMBOL...

DIFFICULTY TO REMEMBER: **HARD**



~44 BITS OF ENTROPY

□□□□□□□□□□
 □□□□□□□□□□
 □□□□□□□□□□
 □□□□□□□□□□

$2^{44} = 550 \text{ YEARS AT } 1000 \text{ GUESSES/SEC}$

DIFFICULTY TO GUESS: **HARD**

THAT'S A BATTERY STAPLE.

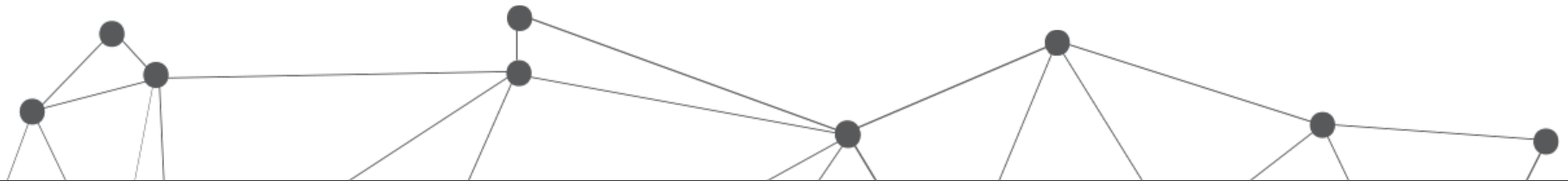
CORRECT!

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.

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





Best Practices



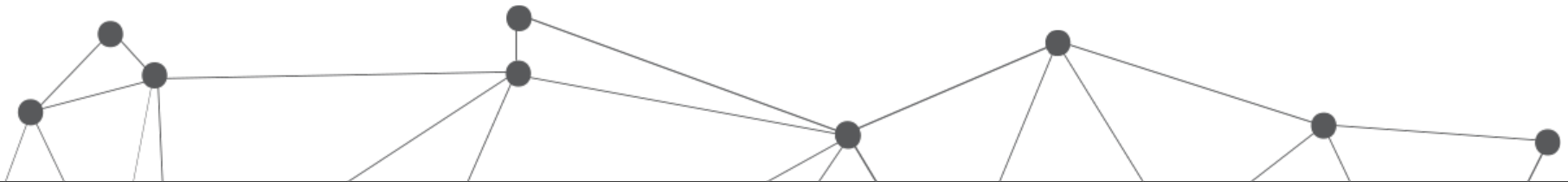


DESIGNERHIPSTER.COM

17-factor authentication

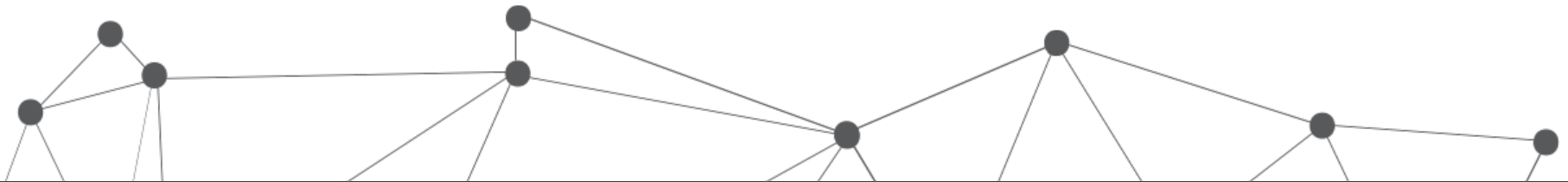
Protect your data

- 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



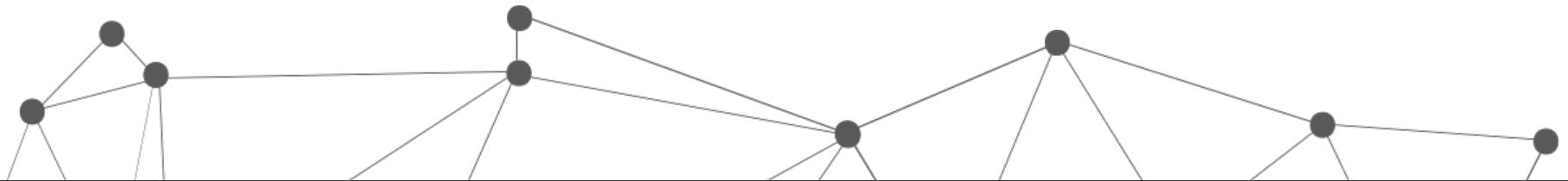
Protect your Network

- 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



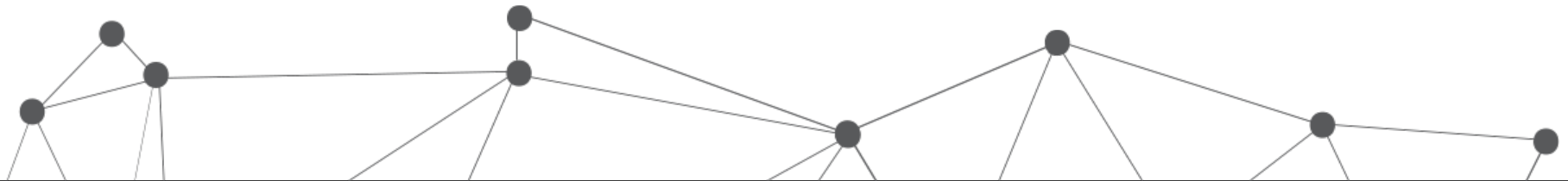
Acceptable Use Policies

- Make sure you have an AUP
 - Make sure your faculty and students receive and agree to it
 - Clearly state the penalties of violation
 - 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.



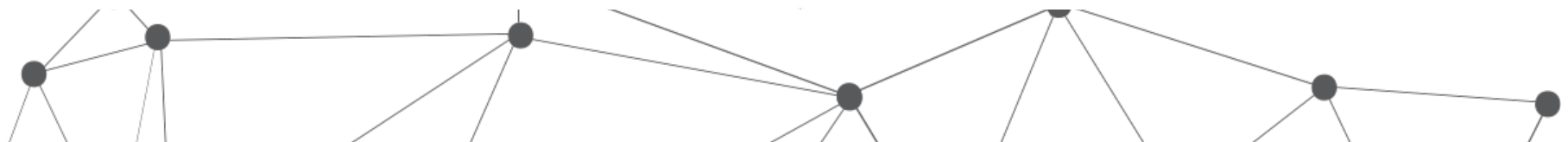
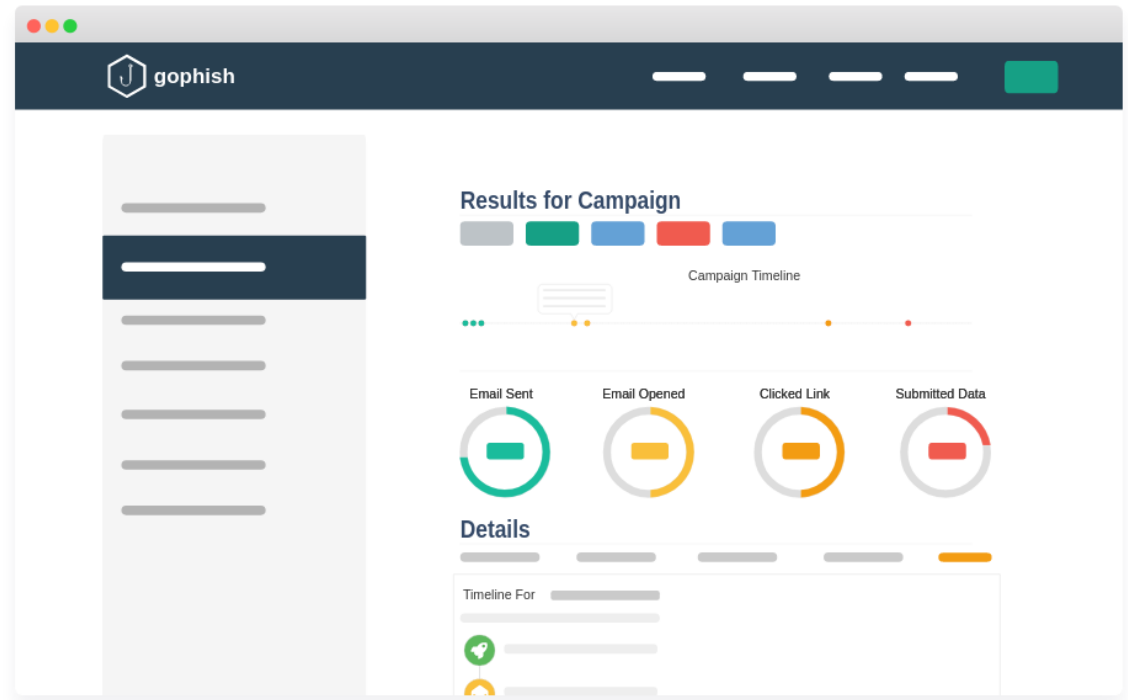
Launch the Campaign

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



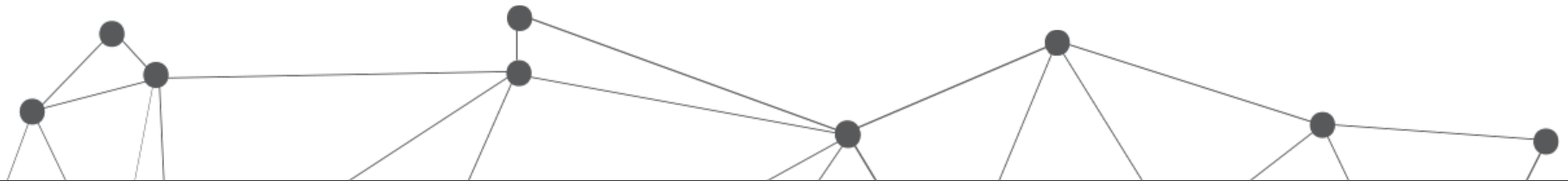
Track Results

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

