Digestible Bites of Cyber Security Awareness – *Security Bytes*, a Case Study

Cheryl Seaman

Stephanie Erickson

WHO ARE WE?

- Federal Team Lead for Policy, Awareness, and Training at NIH

- Training Developer/ Instructional Designer at NIH from Triumph Enterprises

OUR TALK IS ABOUT…

- Ancient Times of Awareness

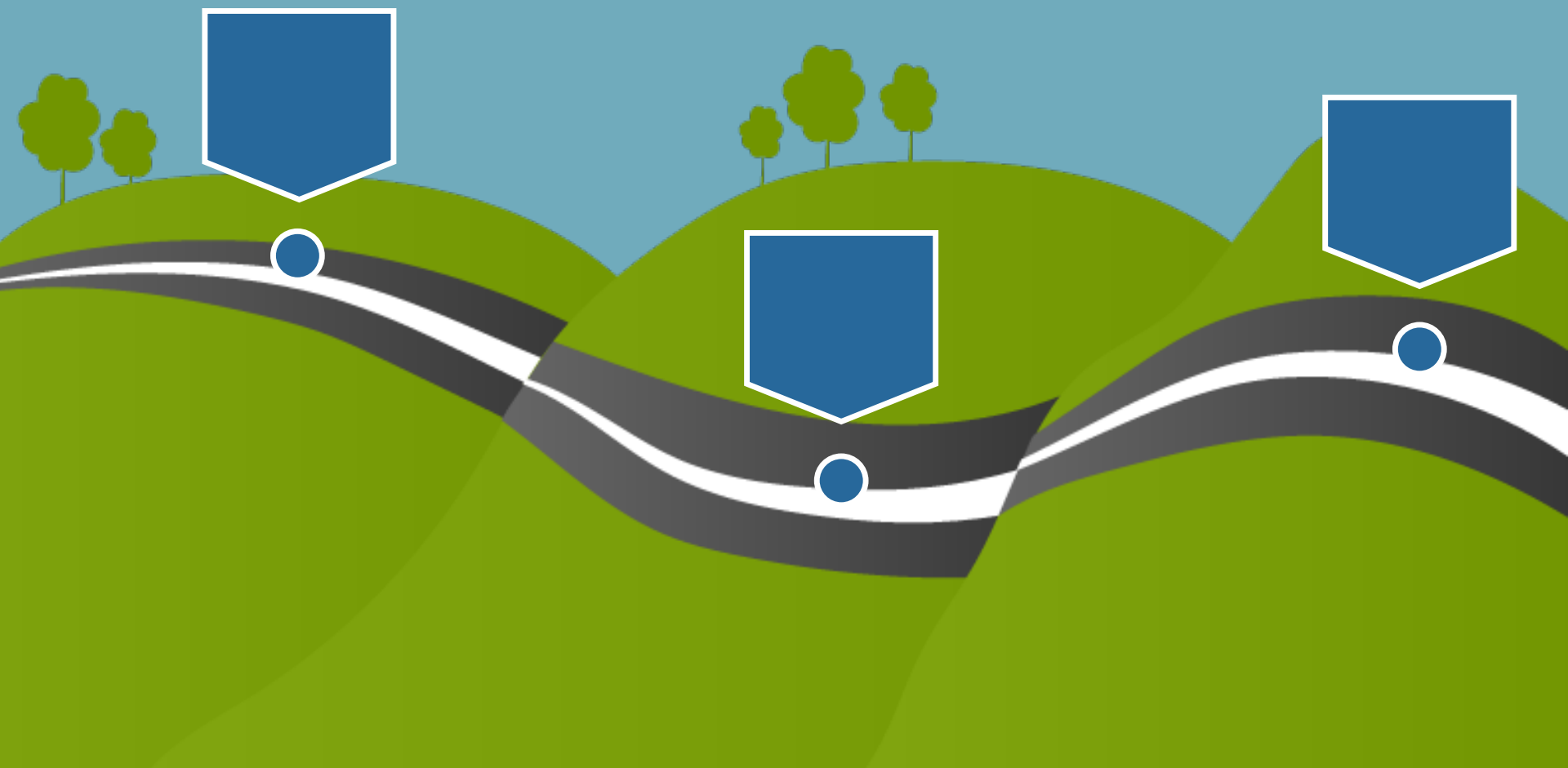
- Dawn of New *Security Bytes*
  - What's a Byte and How do you make one?
  - Taste a Byte *(of Online Identity Theft)*

- Trials and Tribulations
  - Changes
  - Lessons Learned

- How Can You Do It Too

WHERE DID WE COME FROM?

In the Land before Security Bytes…



WHERE DID WE COME

SECURITY BYTES
DIGESTIBLE BITES OF INFORMATION SECURITY AWARENESS

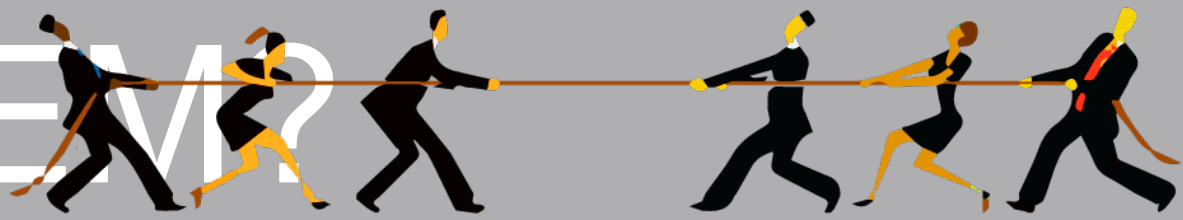
Tips to Help You Practice Safe and Secure Online Shopping From Home

With the holidays approaching, lots of shoppers will be enjoying the convenience and economy of Internet shopping from home.
Here are some useful tips to ensure that your experience is a safe one!

Know who you are dealing with and what you are buying: Almost anyone can set up an online shopping website. Stick to companies you know and trust and make sure you are on the correct website. Don't click on a vendor link in an email that "looks" legitimate because it might take you to a malicious site that will download malicious software or steal financial information. **If an offer looks too good to be true—it's probably a scam!** Watch out for online coupon scams that ask for personal information— Never agree to reveal your personal information just to participate in a promotion.

Pay by credit or charge card because your online transaction will be protected by the Fair Credit Billing Act: This law gives you the right to dispute charges and under certain circumstances withhold payment while your creditor is investigating your claim. If there is an unauthorized charge, you may only be liable for the first $50. Check out the company's online shopping guarantee, warranty, return and/or purchase protection benefits. Review the terms of the purchase and keep a paper trail. Examine your credit card statements and be on the lookout for unauthorized charges.

WHY DO WE DO THEM?

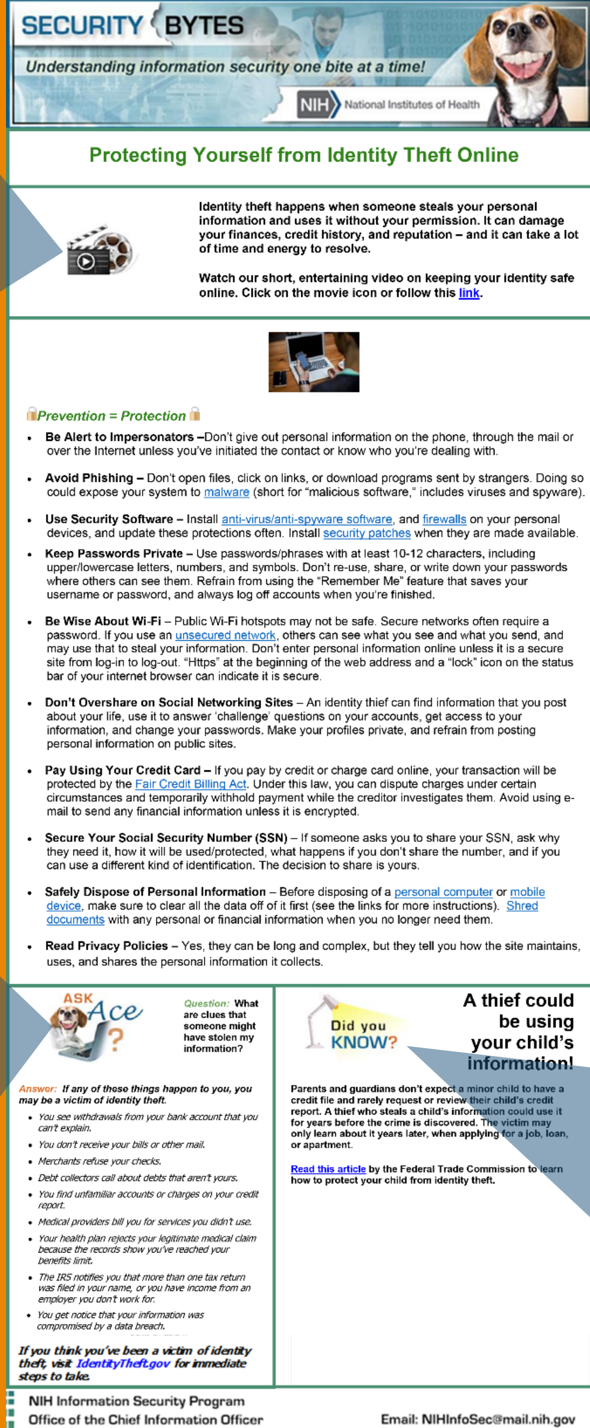


- What do we have working against us?
- What do we have going for us?

SE•CU•RI•TY BYTES

[si-kyoo r-i-tee bahyts]

- 3-Prong Approach
- Edutaining
- Timely
- Easy-to-understand
- Focus on one topic



Protecting Yourself from Identity Theft Online

Identity theft happens when someone steals your personal information and uses it without your permission. It can damage your finances, credit history, and reputation – and it can take a lot of time and energy to resolve.

Watch our short, entertaining video on keeping your identity safe online. Click on the movie icon or follow this link.

Prevention = Protection

- **Be Alert to Impersonators –** Don't give out personal information on the phone, through the mail or over the Internet unless you've initiated the contact or know who you're dealing with.
- **Avoid Phishing –** Don't open files, click on links, or download programs sent by strangers. Doing so could expose your system to malware (short for "malicious software," includes viruses and spyware).
- **Use Security Software –** Install anti-virus/anti-spyware software, and firewalls on your personal devices, and update these protections often. Install security patches when they are made available.
- **Keep Passwords Private –** Use passwords/phrases with at least 10-12 characters, including upper/lowercase letters, numbers, and symbols. Don't re-use, share, or write down your passwords where others can see them. Refrain from using the "Remember Me" feature that saves your username or password, and always log off accounts when you're finished.
- **Be Wise About Wi-Fi –** Public Wi-Fi hotspots may not be safe. Secure networks often require a password. If you use an unsecured network, others can see what you see and what you send, and may use that to steal your information. Don't enter personal information online unless it is a secure site from log-in to log-out. "Https" at the beginning of the web address and a "lock" icon on the status bar of your internet browser can indicate it is secure.
- **Don't Overshare on Social Networking Sites –** An identity thief can find information that you post about your life, use it to answer 'challenge' questions on your accounts, get access to your information, and change your passwords. Make your profiles private, and refrain from posting personal information on public sites.
- **Pay Using Your Credit Card –** If you pay by credit or charge card online, your transaction will be protected by the Fair Credit Billing Act. Under this law, you can dispute charges under certain circumstances and temporarily withhold payment while the creditor investigates them. Avoid using e-mail to send any financial information unless it is encrypted.
- **Secure Your Social Security Number (SSN) –** If someone asks you to share your SSN, ask why they need it, how it will be used/protected, what happens if you don't share the number, and if you can use a different kind of identification. The decision to share is yours.
- **Safely Dispose of Personal Information –** Before disposing of a personal computer or mobile device, make sure to clear all the data off of it first (see the links for more instructions). Shred documents with any personal or financial information when you no longer need them.
- **Read Privacy Policies –** Yes, they can be long and complex, but they tell you how the site maintains, uses, and shares the personal information it collects.

ASK Ace ?

Question: **What are clues that someone might have stolen my information?**

***Answer:* If any of these things happen to you, you may be a victim of identity theft.**

- *You see withdrawals from your bank account that you can't explain.*
- *You don't receive your bills or other mail.*
- *Merchants refuse your checks.*
- *Debt collectors call about debts that aren't yours.*
- *You find unfamiliar accounts or charges on your credit report.*
- *Medical providers bill you for services you didn't use.*
- *Your health plan rejects your legitimate medical claim because the records show you've reached your benefits limit.*
- *The IRS notifies you that more than one tax return was filed in your name, or you have income from an employer you don't work for.*
- *You get notice that your information was compromised by a data breach.*

If you think you've been a victim of identity theft, visit IdentityTheft.gov for immediate steps to take.

Did you KNOW?

A thief could be using your child's information!

Parents and guardians don't expect a minor child to have a credit file and rarely request or review their child's credit report. A thief who steals a child's information could use it for years before the crime is discovered. The victim may only learn about it years later, when applying for a job, loan, or apartment.

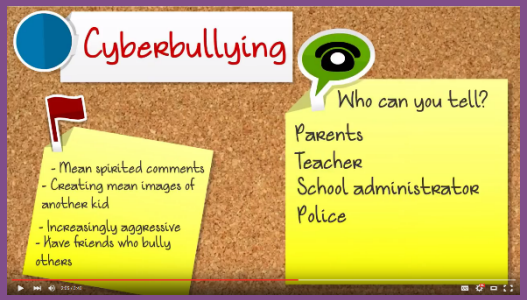
Read this article by the Federal Trade Commission to learn how to protect your child from identity theft.

NIH Information Security Program
Office of the Chief Information Officer
Email: NIHInfoSec@mail.nih.gov

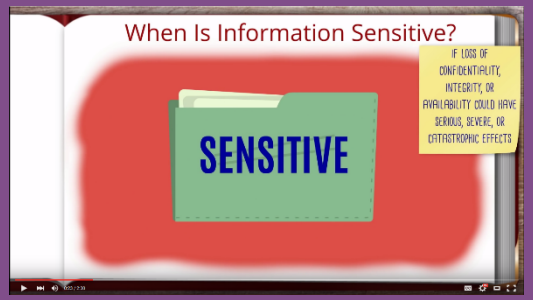
EMAIL

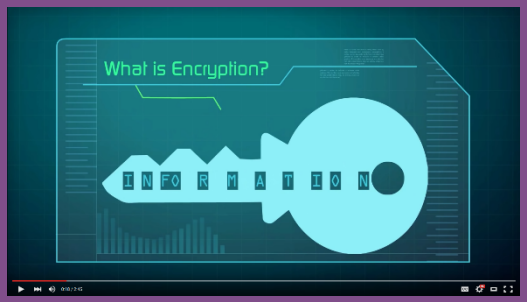
- Mascot
- Visually appealing
- Quick read
- Segmented
- Easy reference

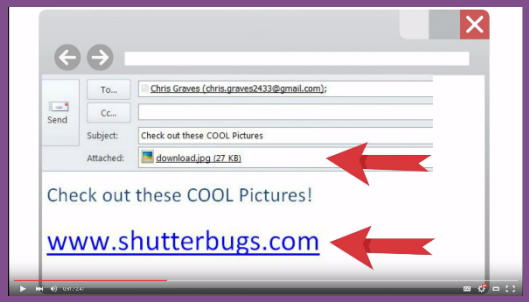
VIDEO


Cyberbullying
- Mean spirited comments
- Creating mean images of another kid
- Increasingly aggressive
- Have friends who bully others
Who can you tell?
Parents
Teacher
School administrator
Police


DELETING...
EMAIL


When Is Information Sensitive?
SENSITIVE
IF LOSS OF CONFIDENTIALITY, INTEGRITY, OR AVAILABILITY COULD HAVE SERIOUS, SEVERE, OR CATASTROPHIC EFFECTS

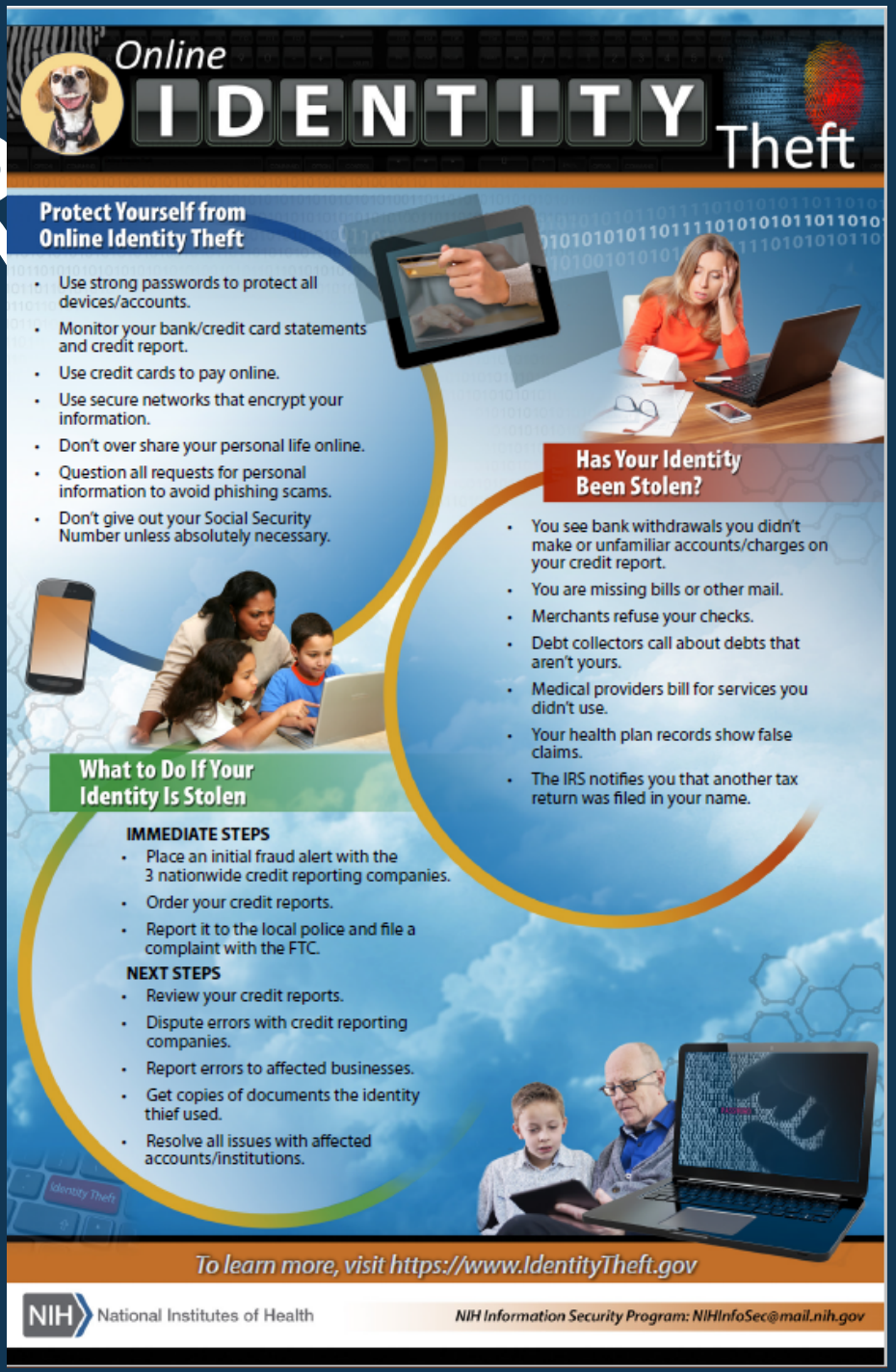

What is Encryption?
INFORMATION


Send
To...
Chris Graves (chris.graves2433@gmail.com);
Cc...
Subject:
Check out these COOL Pictures
Attached:
download.jpg (27 KB)
Check out these COOL Pictures!
www.shutterbugs.com


WOAH THERE LITTLE FELLA!
click here
CLICK HERE!

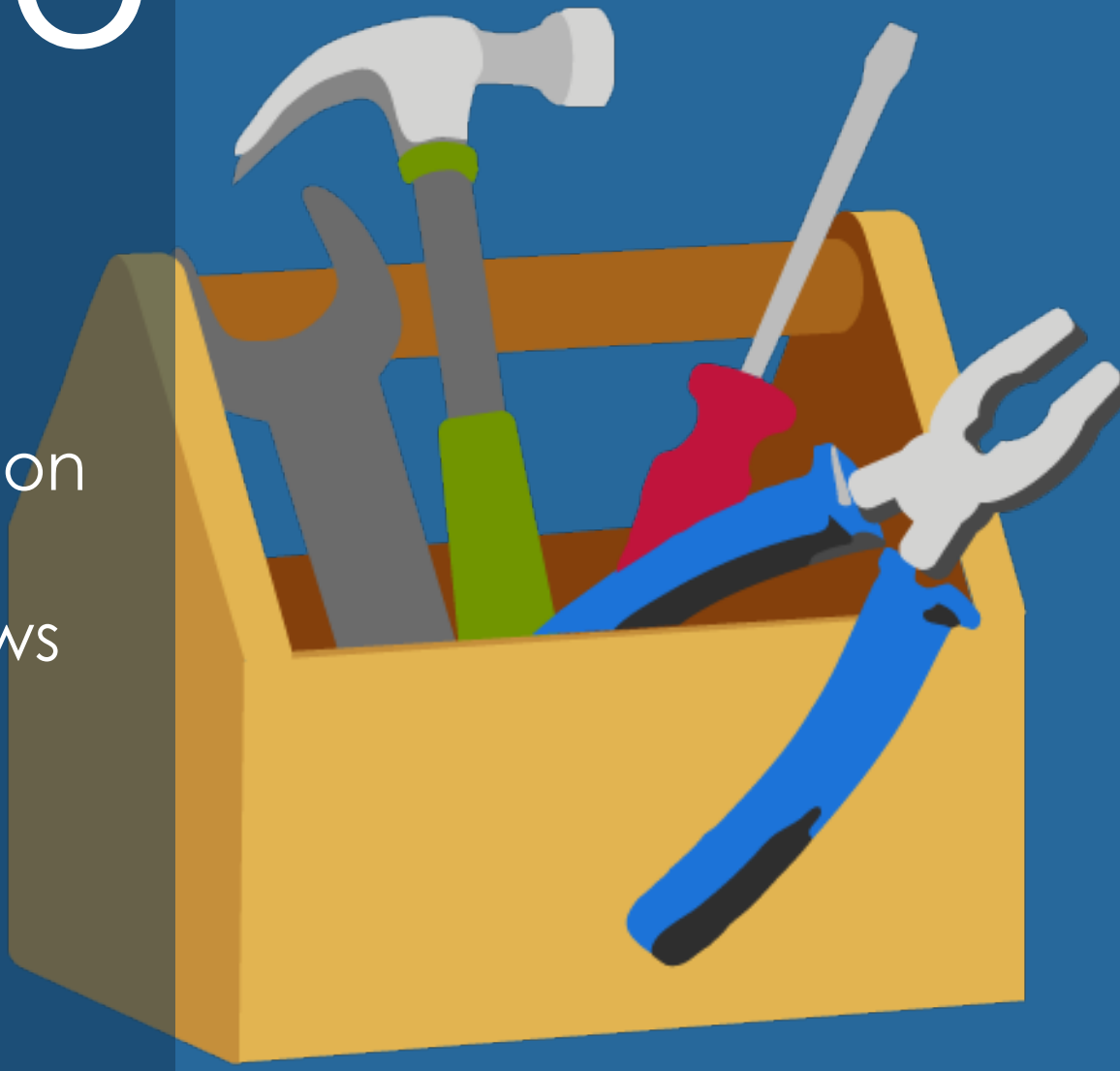
POSTER

- Tabloid size (11x17)
- Cardstock
- Enduring content



HOW DO WE MAKE THEM?

- In house
- Free & subscription software
- Multi level reviews
- Section 508 Compliant

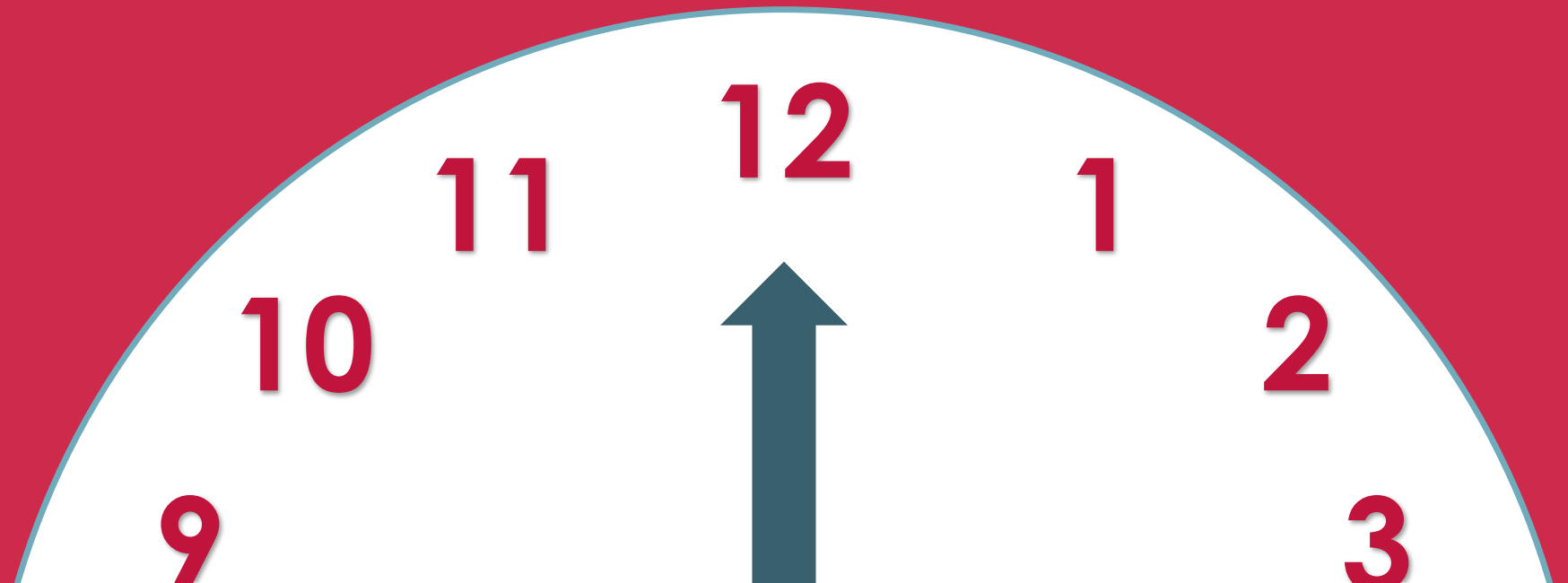


WHO ARE THEY FOR?

- Targeted to NIH users
- Videos publicly available
- Willing to share

WHEN DO WE SEND THEM?

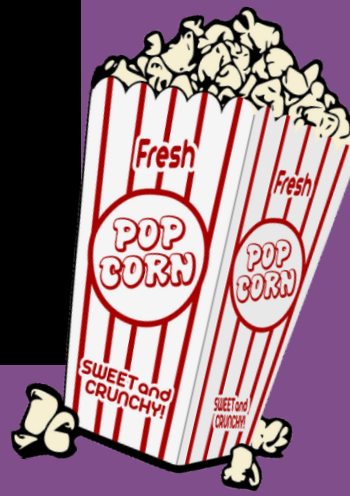
Every other month



DIVE IN

"Protecting Yourself From Identity Theft Online" Security Byte

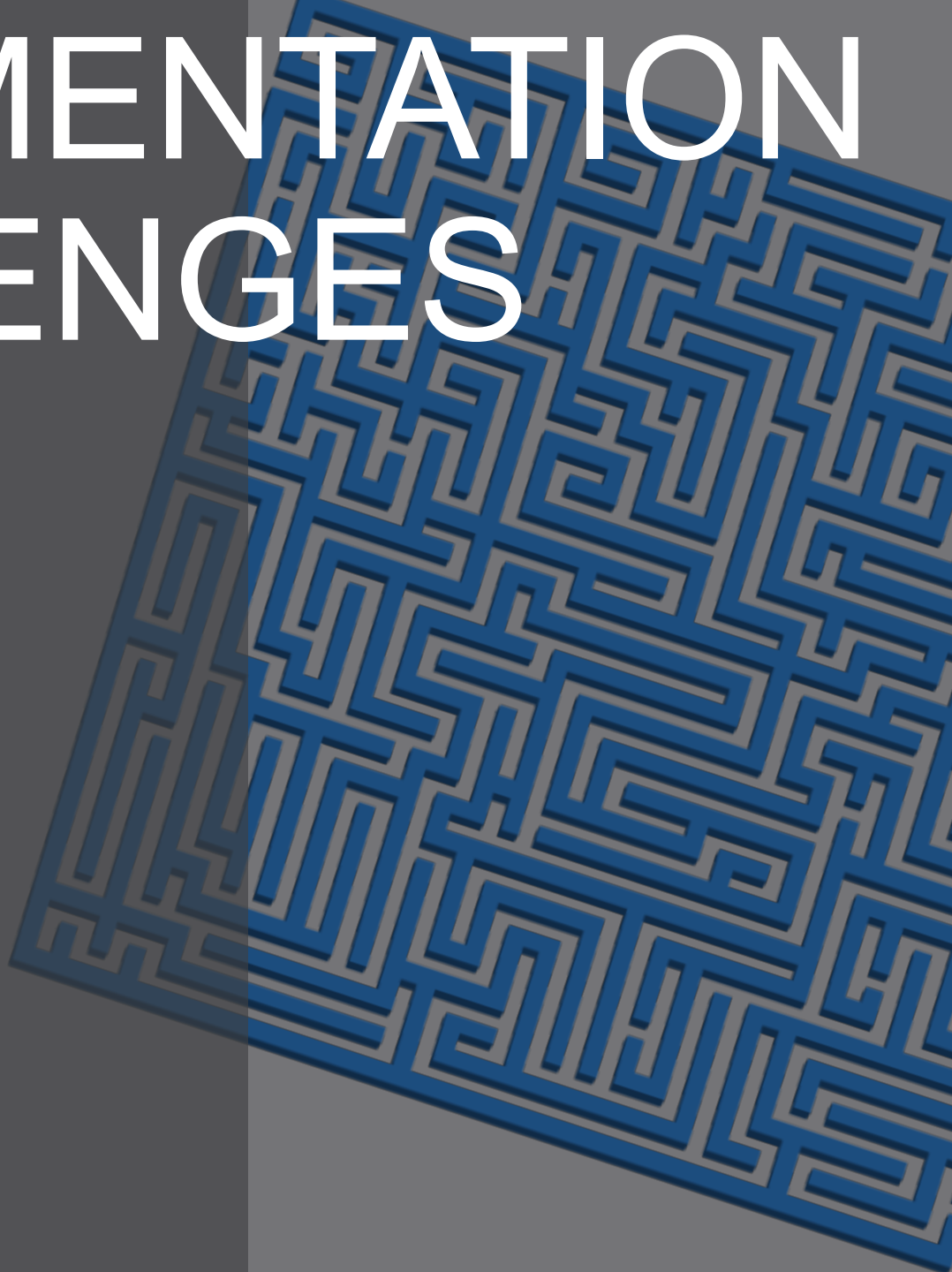
RELAX, AND ENJOY THE



https://youtu.be/UQCzTkzIypU

IMPLEMENTATION CHALLENGES

- Differing email requirements
- Lots of emails daily
- Dependent on individual ISSOs
- Numerous communications schedules
- Inbox “Rules”



ARE WE ON TARGET?

LET'S DO A SURVEY

- Be careful what you ask for

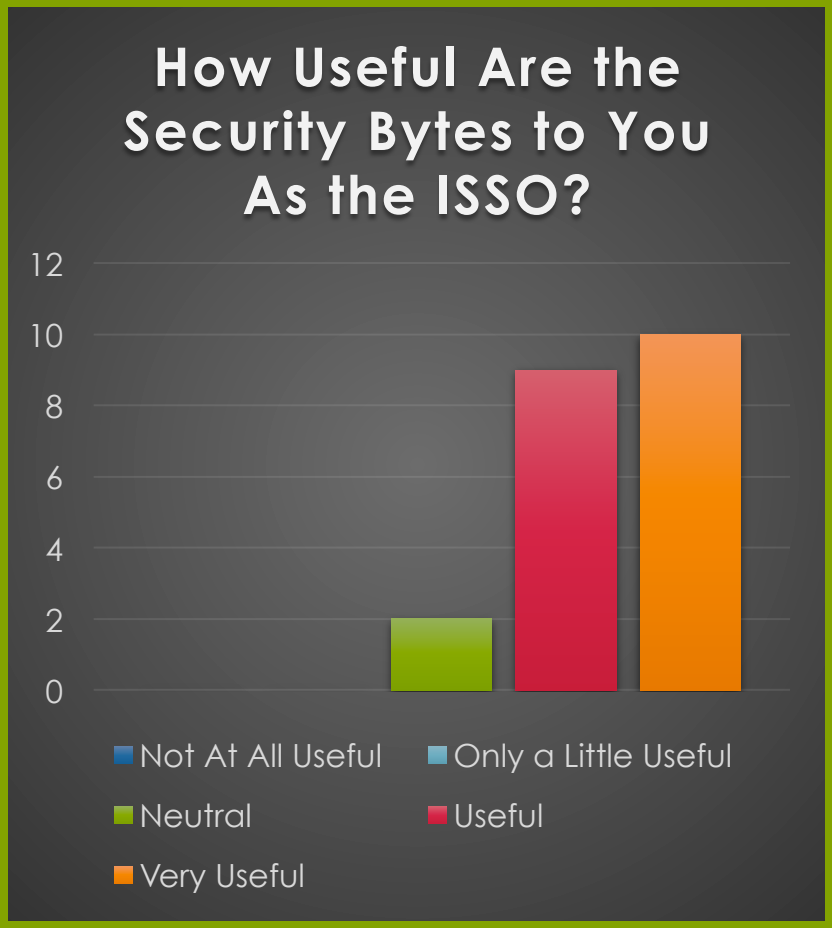
AWARENESS RATINGS

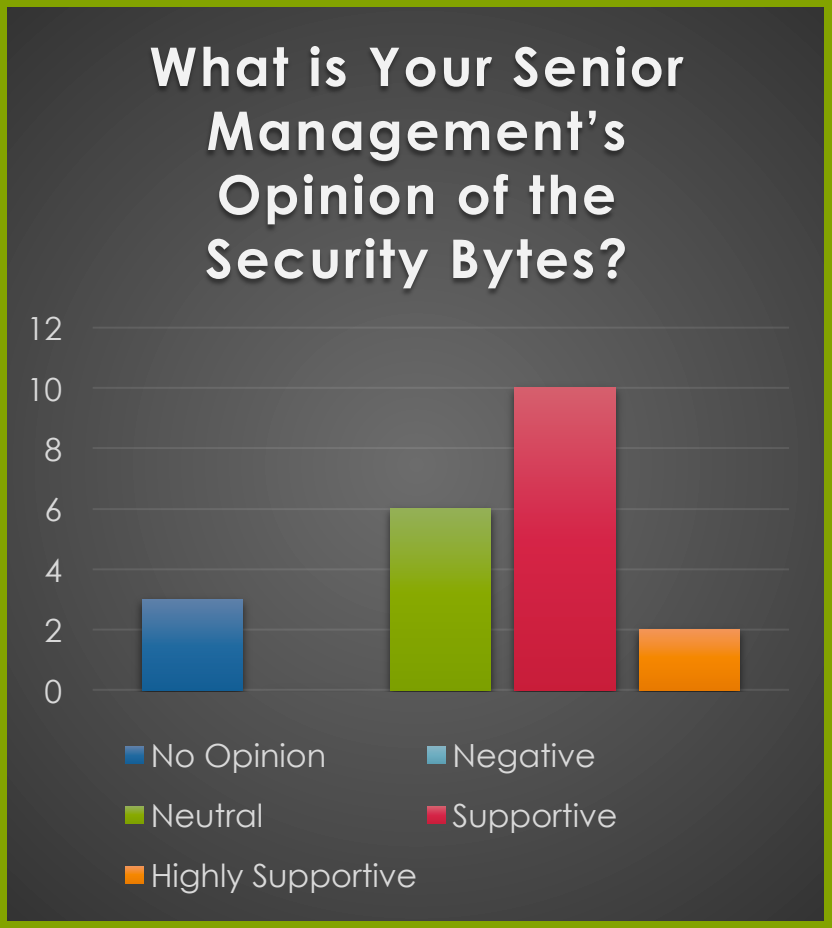
Emails 

Videos 

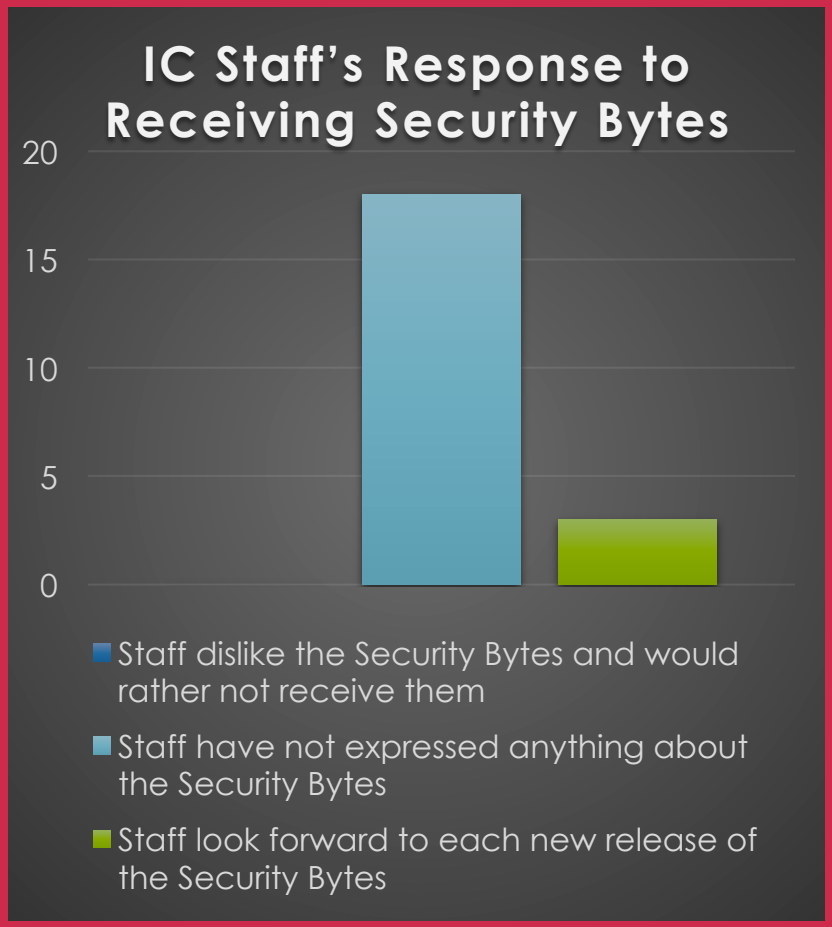
Posters 

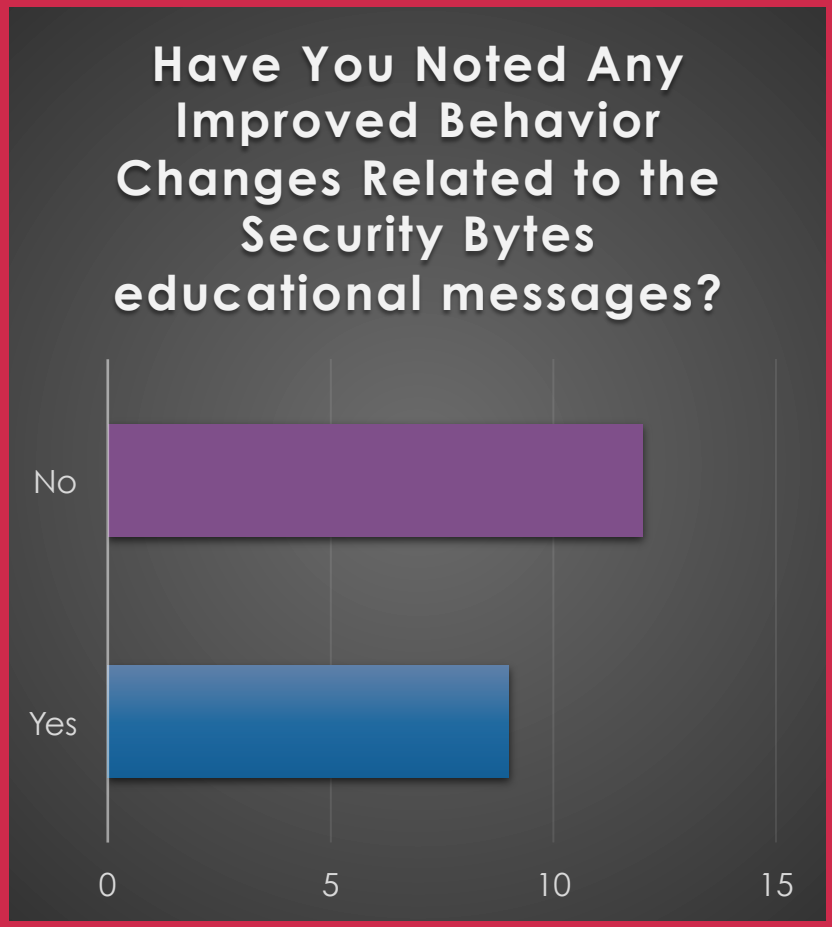
ISSO'S EXPERIENCE





ISSO'S EXPERIENCE

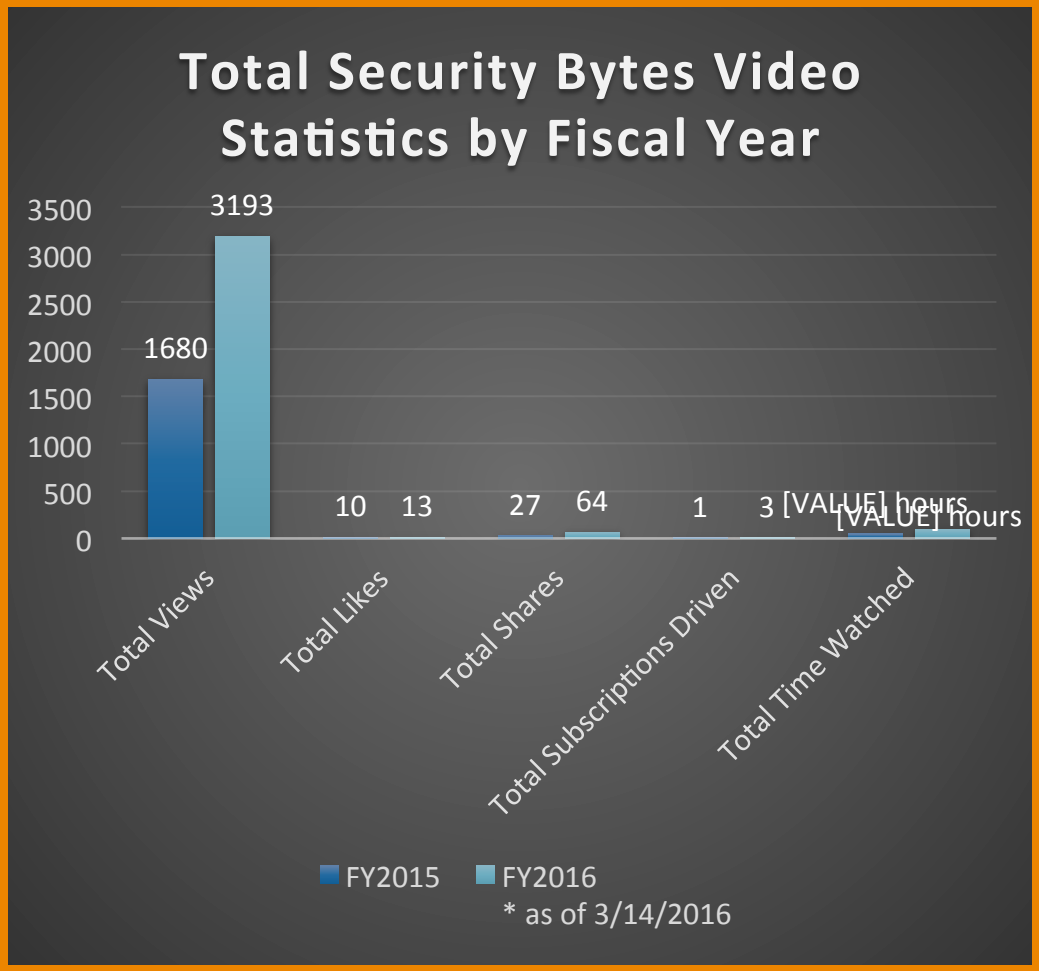




METRICS ON VIDEOS

"Keep up the good work. Especially, the embedded videos."

"We find the videos very helpful and we believe they help our users to better understand the subject."



LESSONS LEARNED

- Review Process
- More ISSO Buy-In
- Continually Refining
- Get Senior Management Support
- ***Marketing is Key!***

HOW CAN YOU DO IT TOO?

IDEAS FOR TOOLS/ RESOURCES

WAYS TO CUSTOMIZE OUR APPROACH TO YOUR ORGANIZATION

AWARENESS GALLERY

- Houses previous releases of *Security Bytes*
- Dedicated topic pages
- Other resources

THANK YOU

NIH Information Security Program
Phone: 301-881-9726
Email: NIHInfoSec@nih.gov
Visit us at: https://ocio.nih.gov/