Creative Writing – how to put more buzz into your stories!

Using 'in the news' topics as a source for your awareness materials

Lab Pack

Cathy Click – FedEx

John Scott – Bank of England

Statistics prove that messages delivered as stories can be up to **22 times** more memorable than just facts. https://www.quantifiedcommunications.com/blog/storytelling-22-times-more-memorable

A good story:

- Organizes abstract material into a meaningful structure
- Engages emotions and triggers an emotional response
- Brain is transported by narrative

Core topics:

In our day jobs, we often cover the same subjects over and over again:

- Password strength
- Password creation/maintenance
- Privacy/family and business
- Data handling
- Patching
- Ransomware
- Email/phishing

How can we approach the same core topics over and over again using current news headlines to keep our readers engaged?

- Individuals hear about digital dangers but can't relate to themselves
- Individuals don't know where to go to find clear details on topics
- No one knows these topics like we do, let's start sharing!

The Answer?

Look for the human – like a hunt for 'Where's Waldo?' find the beginning point.

Ask -

- What happened?
- Who did it?
- How, why and when did it happen?
- Where is Waldo?
- What can I do to keep it from happening to me?

The Plan!

In the following Labs, we're going to cover 3 easy steps to impactful and creative content creation.

1. **Dissect**
2. **Define**
3. **Decorate**

LAB 1: DISSECT

This is a group activity around your table and you have 20 minutes.

You will learn:

How to break down a news story into basic bullets to find the key points that relate to our readers and determine the teachable topics.

You can use:

- The research information on pages 3 - 5
- Your mobile device and web searches
- Your knowledge and the knowledge of the people at your table

You will create:

- Bullet answers to the following questions aimed at a non-technical audience

Lab 1: Questions

In 2017 a Distributed Denial of Services (DDOS) attack was launched using Internet of Things (IoT) devices. Using the supplied materials, the internet and knowledge from others at the table -

a. Define DDOS and IoT

b. How does a DDOS attack work using IoT devices?

c. What was the difference this time from a normal DDOS attack?

d. What Core Topics (Page 1) does this cover?

Lab 1: Resource 1

As IoT use ramps up, so do attacks on networks

https://gcn.com/articles/2018/02/28/iot-network-attacks.aspx

By Peter Martini, Feb 28, 2018

While the public is increasingly aware of the internet-of-things technology all around them, many people remain blind to how vulnerable IoT leaves them to data theft. What's even more concerning is that the threat landscape is maturing, faster than many network administrators can keep pace with.

That's because the distributed denial of service attacks and highly disruptive network shutdowns that characterized IoT hacking in the past are becoming far more targeted and sophisticated. This is especially concerning for major infrastructure projects that leverage IoT tools, as hacks into these networks can leave entire municipal data stores vulnerable to theft.

From "muscle-flexing" to financial gain

In 2016 and 2017, there was a rash of DDoS attacks targeting IoT devices that really started giving cybersecurity experts pause about the rapid adoption of new connected devices.

The Mirai attack was one such DDoS operation that used an army of botnet-infected IoT devices to flood networks like Twitter, GitHub and PlayStation -- just to name a few -- with "loud" network traffic. This drowned out legitimate directives from network administrators attempting to mediate the attack, forcing the servers to shut down as traffic overwhelmed their operations

Closed-circuit TV cameras -- used by both private and public entities -- were the top device compromised in these attacks.

While the Mirai attack caused headaches and ran up hefty bills for remediation at the companies affected, it was largely considered an exercise in showboating. Pras Jha, who pleaded guilty to orchestrating the attack alongside two classmates, was able to make vulnerabilities to IoT networks glaringly obvious. This opened the door up to a new generation of attackers to "one-up" Jha by attacking financial assets, taking advantage of readily available ransomware to exploit poorly secured IoT networks for big pay offs.

Forward-facing protections a must

Many IT teams and network security administrators are already taking exhaustive measures to future-proof their networks for tomorrow's advanced threats. While these teams may be taking stock of the mobile devices, branch offices and remote workers that need protection across their networks.

IoT devices will increase the number of devices by a significant order of magnitude. Even if IT managers are dedicating separate networks for IoT, administrators must use the same diligence in making sure these networks are as manageable as possible. This includes assessing their hardware for security gaps, including weak encryption implementation or inadequate patching functions.

For instance, where encryption is involved, IT teams must ensure that data is encrypted while at rest and in motion. Just relying on full-disk encryption, for instance, will help secure data when a device or server is turned off. But as soon as a user logs on or powers up the technology housing that content, anyone -- including bad actors who entered the network during downtime -- can access that previously encrypted data.

Rather, teams must use encryption at all times, employing solutions that leverage industry standards like SSL to ensure protections are up to date. Equally important -- if not even more so -- is ensuring that encryption keys are stored privately and offline – not within a server with access to the network.

Organizations must also ensure that they are putting defenses at network gateways to stop bad actors from accessing data stores to begin with. This requires teams to take a "defense-in-depth" approach to network security, putting as many layers of protections at network gateways as possible. Just relying on firewalls, for instance, won't suffice as these protections only look at packets of data streaming past the perimeter -- not the whole file. Standard proxies, too, can complement the firewall protections, but they still have their limitations and usually require constant tweaking.

Instead, secure web gateways that fold a consortium of solutions into a single management console can help bring sanity and clarity to an otherwise messy network of interconnected devices. Firewalls, proxies and an array of active defense mechanisms -- from sandboxing to content filtering – can be combined into an effective network gateway to block bad actors from entering the network and leaving with valuable data.

Even the most extensive network security solutions can't thwart every threat -- especially as IoT devices make network security more complicated than ever before. But with risks rapidly growing, organizations would be wise to explore the most extensive defenses possible.

Lab 1: Resource 2

The DDoS Attack Against Dyn: One Year Later

https://www.forbes.com/sites/davelewis/2017/10/23/the-ddos-attack-against-dyn-one-year-later/2/#

Dave Lewis, October 23, 2017

On October 21, 2016, one year ago this past weekend, the customers of a company called Dyn found themselves knocked off the Internet for all intents and purposes. A massive distributed denial of service attack (DDoS) was underway and it had managed to render thousands of websites inaccessible. The attack specifically targeted the domain name servers (DNS) for the provider Dyn (now Oracle).

The initial attack began at 7 am in the morning of Oct 21st. Just over two hours later the attack had been mitigated by the company. This however was not the end of the assault. Two more attacks were launched against the service provider throughout the course of the day. The attack caused millions of Internet users to be unable to connect to numerous websites when the website addresses could not be resolved. This was an unfortunate result.

Through research from Akamai Technologies (*full disclosure, I work there*) and the security firm, Flashpoint, it was disclosed that this attack was facilitated in part with the attackers use of the Mirai botnet [.pdf]. This was a botnet that was built out from a rag tag collection of Internet of Things (IoT) related devices. The botnet was comprised of all manner of internet connected devices from home routers to digital video recorders.

One company whose devices bore the brunt of the Mirai compromise was Hangzhou Xiongmai Technology. Their DVRs were heavily used in Mirai build out.

From PC World:

"Mirai is a huge disaster for the Internet of Things," Xiongmai said in an email to IDG News Service. "(We) have to admit that our products also suffered from hacker's break-in and illegal use."

How was a botnet like Mirai possible? In most cases the IoT devices that were conscripted into the Mirai botnet had default credentials stored. These default credentials allowed the attackers to compromise the devices in a simple manner. In point of fact, there were default credentials for some 60+ devices found in the source code for Mirai that was dumped online several days after the initial attacks.

The curious aspect of these attacks was that there were no claims of responsibility at first. The next day after the attacks the first of several groups claimed credit for the incident. The group calling themselves, "New World Hackers" were followed by claims from Anonymous and Spainsquad. None of the aforementioned attacks were subsequently validated.

Lab 1: Resource 3

all_secure@fedex eNewsletter

February 2017
Vol. 16 No. 1

STOP. THINK. CONNECT.

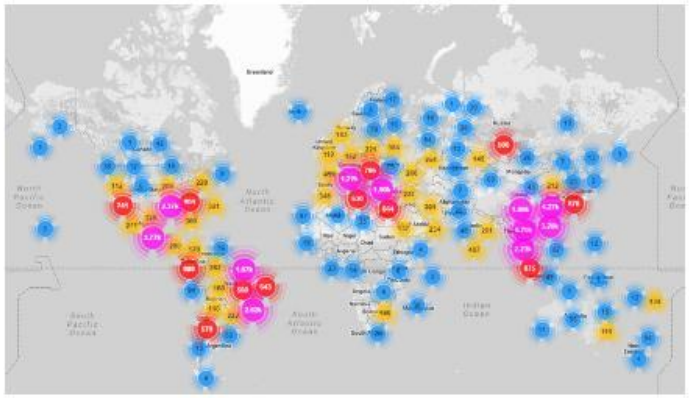
IS YOUR HOME A SAFE HOUSE FOR CYBER CRIMINALS?

ARE YOU HARBORING ZOMBIE ATTACK DEVICES?

October 21, 2016, the Internet ground to a crawl. A distributed-denial-of-service (DDoS) attack had been launched against Dyn, a domain registrar host. Dyn customers, including Twitter, Etsy, Github, Vox, Spotify, Airbnb, Netflix, and Reddit were feeling the effect, as their customers were unable to connect.

This wasn't the first time that this type of DDoS attack had been made. Investigations would reveal that Brian Krebs, American journalist and investigative reporter, had been hit with the same type of attack just 30 days prior on September 20, 2016. Previous to these two attacks, smaller practice sessions had been tested as early as August of 2016.

DDoS attacks are not unusual in the cyber world, but the method these two attacks used were very different from previous DDoS attacks. These attacks utilized malware, Mirai, that was installed on unprotected Internet of Things (IoT) devices.



This map shows the location and number of IoT devices infected with Mirai, creating a global army of zombies. These devices can be called into action at any time for a DDoS attack unless owners take steps to disable hacker access. Enabled UPnP and default device passwords allowed this army of Mirai zombies to be built.

Mirai searches the Internet for known default usernames and passwords on selected devices. And this threat becomes even greater as new IoT devices are connected to the Internet without proper security measures.

Further investigation of the October attack revealed 49,657 unique IPs available in 164 different countries, 100,000 hosted Mirai-infected devices* were called to work in unison to cripple Dyn. This issue of *all_secure@fedex* will discuss a few ways that team members can keep their IoT devices from being called to action in future DDoS attacks and protect their personal network.

*http://www.zeedtech.com/blog/a-massive-ddos-attack-came-just-100000-hacked-iot-devices

DID MY LIGHT BULB BREAK THE INTERNET?

No, your IoT light bulb has even less power than the Kardashians for breaking the Internet. More memory is need for the Mirai malware to work, although your closed circuit security cameras (CCTV cameras) may have participated. CCTV cameras, DVRs and routers were the most popular devices used in these attacks.

The most used devices in the October attack, with unchanged user name and passwords, were -

ACTi IP Camera
ANKO Products DVR
Axis IP Camera, et all
Mobotix Network Camera
Packet8 VOIP Phone et. Al
Panasonic Printer

KEEP OUT HACKER ACCESS TO YOUR ROUTER

It is important to change the default password on your router. Hackers sniff the Internet for routers that still have the default ID and password to gain access to your devices and your information.

Consult your router's operating manual before performing any kind of reset procedure, and always follow proper safety precautions indicated in your router's documentation. Directions can vary by make and model of the router. This is an overview of what you need to do to change the default password on your router.

If you know your router's password but just don't know how to change it, you can skip steps 1 and 2 and enter the admin user name and password that you have into step 4. This will allow you to change your wireless router's password without wiping out all your other router's settings.
You will have to change all your routers settings, such as your wireless network SSID, password, encryption settings, etc, after performing this step.

1. If you don't know what your default password is - press and hold the reset button on the back of your wireless router. PLEASE NOTE: The first step in this process will wipe out all of your router's configuration settings and set them back to their out-of-the-box factory defaults.

   You will probably have to hold the reset button from 10 to 30 seconds depending on your brand of router. If you hold it for too short a time it will simply reset the router but won't revert back to its factory default settings. On some routers you may have to use a pin or thumbtack to press the button if it is recessed inside the router.

2. Connect a computer to one of your router's Ethernet ports (These ports are alternatively called jacks or sockets. Ethernet ports accept cables with RJ-45 connectors, but not the one that says WAN)

   Most routers have a web browser-accessible administrator page that you must log in

LAB 2: DEFINE

This is a group activity around your table and you have 30 minutes.

You will learn:

How to use the skills from Lab 1 to find the points of interest and teachable topics, and then use those to create a readable and engaging summary.

You can use:

- The research information on pages 7-9
- Your mobile device and web searches
- Your knowledge and the knowledge of the people at your table

You will create:

- Bullet answers to the following questions aimed at a non-technical audience
- A call to action – What can I do to keep it happening to me?
- A user friendly paragraph and headline

Lab 2: Questions

In 2017 a ransomware attack called NotPetya hit many businesses. This ransomware attack had a larger impact than many because of the way was created to spread. Using the supplied materials, the internet and knowledge from others at the table -

a) Develop bullet summaries of the story as in Lab 1

b) Answer the question: "What can I do to keep it from happening to me?"

c) Write a headline and a single paragraph for a newsletter on NotPetya

Lab 2: Resource 1

Petya ransomware and NotPetya malware: What you need to know now

https://www.csoonline.com/article/3233210/ransomware/petya-ransomware-and-notpetya-malware-what-you-need-to-know-now.html

Josh Fruhlinger, Oct 17, 2017

Petya and NotPetya

NotPetya superficially resembles the Petya ransomware in several ways, but there are a number of important ways in which it's different, and much more dangerous.

Petya and NotPetya are two related pieces of malware that affected thousands of computers worldwide in 2016 and 2017. Both Petya and NotPetya aim to encrypt the hard drive of infected computers, and there are enough common features between the two that NotPetya was originally seen as just a variation on a theme. But NotPetya has many more potential tools to help it spread and infect computers, and while Petya is a standard piece of ransomware that aims to make few quick Bitcoin from victims, NotPetya is widely viewed as a state-sponsored Russian cyberattack masquerading as ransomware.

What is Petya?

Petya is *ransomware* — a form of malware that infects a target computer, encrypts some of the data on it, and gives the victim a message explaining how they can pay in Bitcoin to get the keys to get their data back. The name derives from a satellite that was part of the sinister plot in the 1995 James Bond film *GoldenEye;* a Twitter account suspected of belonging to the malware's author used a picture of actor Alan Cumming, who played the villain, as its avatar.

The initial version of the Petya malware, which began to spread in March of 2016, arrives on the victim's computer attached to an email purporting to be a job applicant's resume. It's a package with two files: an image of young man (supposedly of the job applicant, but actually a stock image) and an executable file, often with "PDF" somewhere in the file name. The plan is to get you to click on that file, and to subsequently agree to the Windows User Access Control warning that tells you that the executable is going to make changes to your computer. (Petya only affects Windows computers.)

How Petya works

If you make the extremely bad decision to agree to this request, Petya will reboot your computer. You'll see what looks like the standard Windows CHKDSK screen you expect to see after a system crash. In fact, the malware is already working behind the scenes to make your files unreachable. What earned Petya the description "the next step in ransomware evolution" despite its initially unimpressive infection rate is the way it encrypts your files. Rather than searching out specific files and encrypting them, like most ransomware does, it installs its own boot loader, overwriting the affected system's master boot record, then encrypts the master file table, which is the part of the filesystem that serves as sort of a roadmap for the hard drive. In essence, your files are still there and still unencrypted, but the computer can't access the part of the filesystem that tells it where they are, so they might as well be lost. At this point, the ransomware demands a Bitcoin payment in order to decrypt the hard drive.

As noted, in order to perform this kind of high-level bad behavior, Petya needs the user to gullibly agree to give permission to make admin-level changes. A couple of months after Petya first began to spread, a new version appeared that was bundled with a second file-encrypting program, dubbed Mischa. Mischa kicks in if the user denies Petya admin-level access; it's only a garden-variety piece of ransomware, just encrypting individual files. (Unusually, it also encrypts .exe files, which may end up interfering with the victim's ability to pay the ransom.)

Petya/NotPetya

Petya was thus at first just another piece of ransomware, with an unusual twist in how it encrypted files. But in June of 2017 that all changed radically. A new version of the malware began spreading rapidly, with infection sites focused in Ukraine, but it also appeared across Europe and beyond. The new variant spread rapidly from computer to computer and network to network without requiring spam emails or social engineering to gain administrative access; the radical advances in its capabilities led Kaspersky Lab to dub it NotPetya, a name that stuck.

Lab 2: Resource 1 (Continued)

NotPetya virus

The NotPetya virus superficially resembles Petya in several ways: it encrypts the master file table and flashes up a screen requesting a Bitcoin ransom to restore access to the files. But there are a number of important ways in which it's different, and much more dangerous:

NotPetya spreads on its own. The original Petya required the victim to download it from a spam email, launch it, and give it admin permissions. NotPetya exploits several different methods to spread without human intervention. The original infection vector appears to be via a backdoor planted in M.E.Doc, an accounting software package that's used by almost every company Ukraine. Having infected computers from Medoc's servers, NotPetya used a variety of techniques to spread to other computers, including EternalBlue and EternalRomance, two exploits developed by the United States NSA to take advantage a flaw in the Windows implementation of the SMB protocol. It can also take advantage of a tool called Mimi Katz to find network administration credentials in the infected machine's memory, and then use the PsExec and WMIC tools built into Windows to remotely access other computers on the local network and infect them as well.

NotPetya encrypts everything. The NotPetya malware goes far beyond the original Petya trick of encrypting the master boot record, going after a number of other files to seriously screw up your hard drive.

NotPetya isn't ransomware. This is in fact the most shocking — and important — thing about NotPetya. It looks like ransomware, complete with a screen informing the victim that they can decrypt their files if they send Bitcoin to a specified wallet. For Petya, this screen includes an identifying that they're supposed to send along with the ransom; the attackers use this code to figure out which victim just paid up. But on computers infected with NotPetya, this number is just randomly generated and would be of no help in identifying anything. And it turns out that in the process of encrypting the data, NotPetya damages it beyond repair.

So what's NotPetya's real purpose? The fact that it saw an abrupt and radical improvement in efficiency over its Petya ancestor implies a creator with a lot of resources — a state intelligence or cyberwarfare agency, say. That, combined with the 2017 attack's focus on the Ukraine, caused many to point their finger at Russia, with whom Ukraine has been involved in a low-level conflict since the occupation of Crimea in 2014. This accusation was taken up by the Ukrainian government itself, and many Western sources agree, including the U.S. and U.K.; Russia has denied involvement, pointing out that NotPetya infected many Russian computers as well.

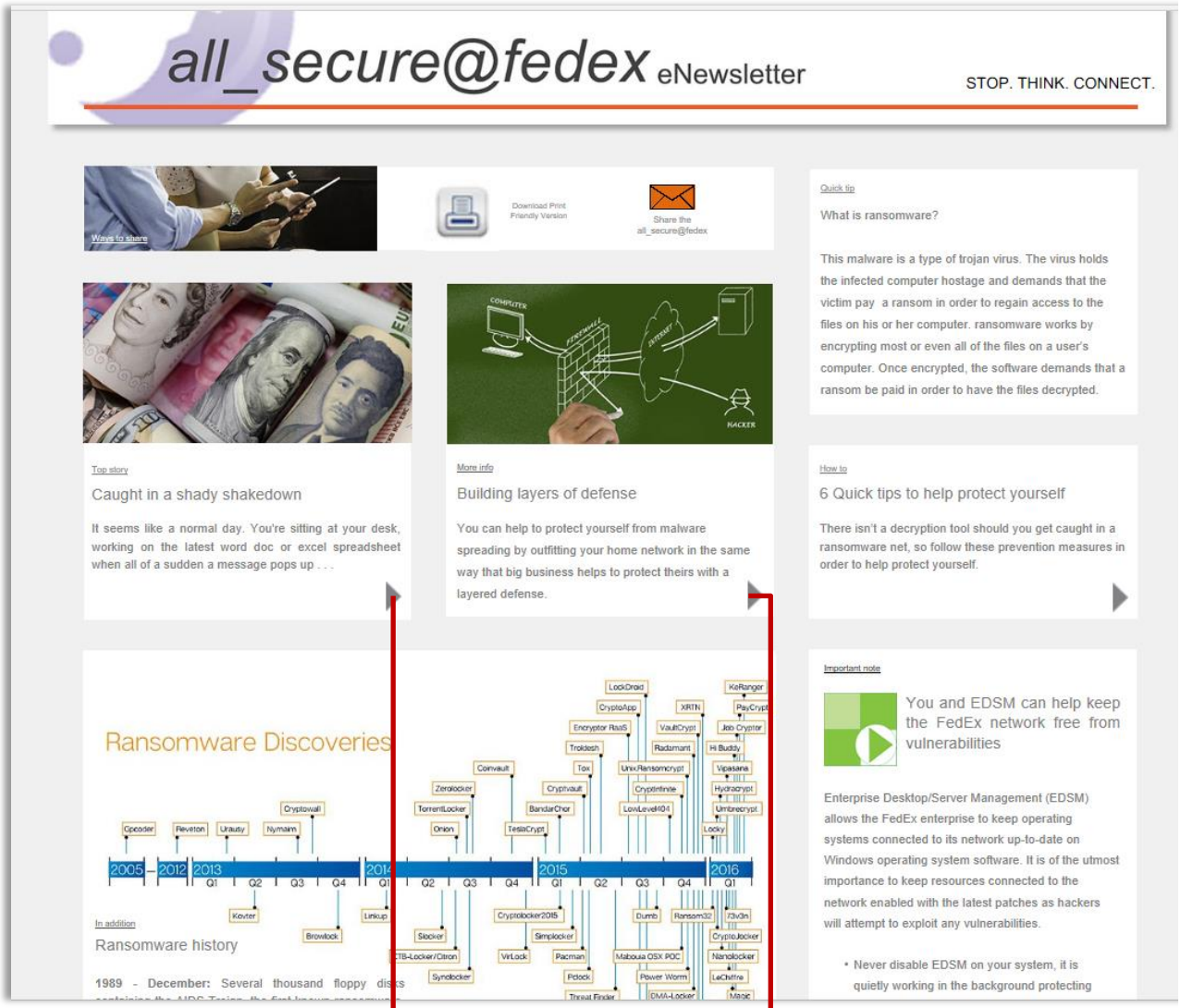
Petya Microsoft patch

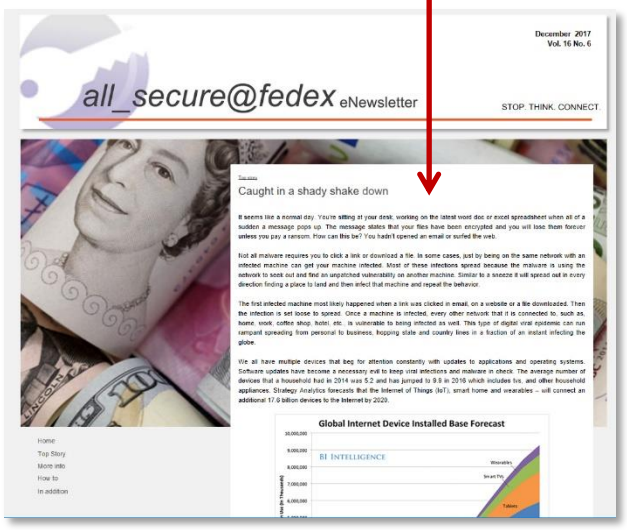
The most important vulnerability to patch to avoid infection by the NotPetya variant is the SMB flaw exploited by EternalBlue. This hole can be patched by MS17-010, which was actually available in March of 2017, several months before the NotPetya outbreak. Still, despite the fact that that the widely publicized WannaCry outbreak, which occurred just weeks before NotPetya hit and exploited the same hole, brought widespread attention to the MS17-010's importance, there were still enough unpatched computers out there to serve as an ecosystem for NotPetya to spread.

Petya and Windows 10

Many of the computers infected by NotPetya were running older versions of Windows. Microsoft says that Windows 10 was particularly able to fend of NotPetya attacks, not just because most installs auto-updated to fix the SMB vulnerability, but because improved security measures blocked some of the other ways NotPetya spread from machine to machine.

Lab 2: Resource 2





LAB 3: DECORATE

This is a group activity around your table and you have 40 minutes.

You will learn:

How to use the skills from Lab 1 and Lab 2 to find the points of interest and teachable topics, and then use those to create a readable and engaging summary. You will identify how to stop it happening to the reader. You'll then create headlines, email subject lines, ideas for graphics and photos to grab the reader's attention.

You can use:

- The research information on pages 11-13
- Your mobile device and web searches
- Your knowledge and the knowledge of the people at your table

You will create:

- Bullet answers to the following questions aimed at a non-technical audience
- A call to action – What can I do to keep it happening to me?
- A user friendly paragraph summary
- Attention grabbing headlines

Lab 2: Questions

In 2017 a ransomware attack called NotPetya hit many businesses. This ransomware attack had a larger impact than many because of the way was created to spread. Using the supplied materials, the internet and knowledge from others at the table -

a) Develop bullet summaries of the story as in Lab 1

b) Answer the question: "What can I do to keep it from happening to me?"

c) Write a single paragraph for a newsletter on the Facebook data breach

d) Come up with the most attention grabbing headline for the story.

Lab 3: Resource 1

Facebook to contact 87 million users affected by data breach

https://www.theguardian.com/technology/2018/apr/08/facebook-to-contact-the-87-million-users-affected-by-data-breach

Nadeem Badshah, Sun 8 Apr 2018 23:40 BST

Message will reveal which users had personal information was harvested by Cambridge Analytica

Eighty-seven million Facebook users around the world will find out on Monday if their details were shared with Cambridge Analytica in one of the social network's largest data breaches.

The firm said affected users would receive a detailed message on their news feeds. The majority of those whose information was shared with the data analytics firm – about 70 million – are in the US.

More than 1 million people in each of the UK, Philippines and Indonesia may also have had their personal information harvested as well as 310,000 Australian Facebook users.

All 2.2 billion Facebook users will receive a notice titled "Protecting Your Information" with a link to see what apps they use and what information has been shared with those apps. They will be able to shut off apps individually or turn off third-party access.

It comes after the Observer revealed that Cambridge Analytica, which worked with Donald Trump's election team, acquired millions of profiles of US citizens and used the data to build a software program to predict and influence voters.

Facebook discovered the information had been harvested in late 2015 but failed to alert users at the time.

The information was collected through an app called thisisyourdigitallife, built by the Cambridge University academic Aleksandr Kogan in collaboration with Cambridge Analytica.

Hundreds of thousands of users were paid a fee to take a personality test and consented to have their data collected. The app also harvested information about the participants' friends.

Facebook's CEO, Mark Zuckerberg, who is expected to testify before Congress this week, acknowledged that he made a "huge mistake" in failing to take a broad enough view of the company's responsibilities.

Facebook's CEO, Mark Zuckerberg, who is expected to testify before Congress this week, acknowledged that he made a "huge mistake" in failing to take a broad enough view of the company's responsibilities.

Cambridge Analytica whistleblower Christopher Wylie previously estimated that more than 50 million people were compromised by the personality test.

In an interview aired on Sunday on NBC's Meet the Press, Wylie said the true number could be even higher than 87 million. He said: "I know that Facebook is now starting to take steps to rectify that and start to find out who had access to it and where it could have gone, but ultimately it's not watertight to say that, you know, we can ensure that all the data is gone forever."

Last month, he told the Observer: "We exploited Facebook to harvest millions of people's profiles. And built models to exploit what we knew about them and target their inner demons. That was the basis the entire company was built on."

Zuckerberg said Facebook came up with the 87 million figure by calculating the maximum number of friends that users could have had while Kogan's app was compiling data.

Cambridge Analytica insisted last week that it had information for only 30 million Facebook users.

Lab 3: Resource 2

Why the recent Facebook/Cambridge Analytica data "breach" matters for students

Sara Mohammed, Ph.D., June 6, 2018

When 80 million Facebook users' data were found to be in the hands of Cambridge Analytica, users of the social media platform–and Congress–decided it was time to take a closer look at the data collected by the platform and the apps it hosts. I couldn't help but draw a parallel to the 50 million public students across the nation whose data are similarly collected and shared by and among numerous entities including (as in the Facebook case) researchers and third-party developers.

Educational data are routinely used in schools for a variety of purposes, such as accountability reporting, planning, communications, and personalizing learning for students. When the right stakeholders have access to the right data at the right time, students benefit. However, we need to be careful–more careful than we have been–to ensure that our students' privacy is protected and their data are used for good.

Today, most if not all students in public and other school systems across the country have some form of data about themselves and their academic progress collected and stored. In 2017, 72 percent of teachers reported using educational data for instructional purposes, and 62 percent of administrators identified data use as a priority for professional development in their district. This information is virtually all collected and/or stored electronically. In 2015, over $13 billion was spent by school districts on ed tech, and as ed tech proliferates, the number and type of agencies that have access to those data only grows. The students in your own life probably have multiple pieces of educational data stored in multiple places, regardless of the community that you live in or the schools they attend–and if they don't currently, they certainly will in the near future.

The primary relevance Facebook data have to educational data is the matter of stewardship. Many individuals in a variety of roles are given the responsibility of "protecting" data (and thereby students' privacy), but few are actually given any authority, much less incentive and support, to do so.

In the case of student data, there are three primary stewards of educational data, depending on the specific context in which those data are being collected and used.

1. The school system (or systems) in which the student is enrolled are primary data stewards.
2. If students or educators use ed tech, then developers, often housed within publishing companies or vendors, are "secondary" stewards of some educational data.
3. If students are participating in any research, evaluation, or measurement activities, researchers along with research institutions (in most cases) can also be secondary stewards of some educational data.

As we saw with the Facebook data, having multiple groups responsible for protecting individuals' data and privacy can, in fact, lead to a situation where no group is sufficiently alert to how data are being shared and used. In other words, misuse of data is unlikely to be detected because each group trusts the other group(s) to be vigilant, so that no group is routinely and regularly checking who has what data and how they are being used.

Several federal laws govern the use and sharing of educational data: FERPA, HIPAA (in the case of data about disabilities), COPPA, and PPRA. The primary problem lies in the enactment and enforcement (or lack thereof) of these laws. Many folks who fall under the jurisdiction of these laws are not aware that they should be following them or don't know what the laws require, and all too often the laws are not enforced. Moreover, while these laws (FERPA in particular) provide critical, necessary, and basic protections to students, they do not go as far as one would reasonably assume. There are misuses of educational data and data sharing that may be considered unethical that are perfectly legal. For example, a company could use educational data that it legitimately collected as part of instruction to target marketing of services or other apps to particular students, schools, or districts.

Lab 3: Resource 2 (Continued)

Fortunately, there are ethical guidelines–such as requiring data collection from students to be for the purpose of improving learning–for collecting and storing any data from individuals for research purposes. These guidelines are administered through Institutional Review Boards (IRBs). These guidelines work in tandem with protective practices that researchers routinely use to safeguard data privacy. These practices include working only with data that have been stripped of personally identifying information (like names or dates of birth), not including groups of individuals who have unique enough information that make their data identifiable (e.g., those from a very uncommon ethnic group), and storing both signed consent forms and data in secured (digital and physical) locations, but separately from each other.

Unfortunately, there are many other purposes for data use that IRBs would not rationally apply to, and these uses do not have nearly as much of an established code of ethics for use. Further, IRBs do not (and are not required to) exist at every entity that conducts research, nor are they used by everyone conducting educational research. Like the laws, enforcement of ethical guidelines is also weak and left only up to the willing to serve as enforcers. Some academic journals and funders of educational research will require their grantees to certify that any data collection they fund is conducted with IRB approval. Occasionally, districts and agencies providing the data will require IRB approval. By and large, the ethical use of educational data is not legislated, and is generally left to up an "honor code."

I view the Facebook data situation as a wake-up call for all of us who generate, collect, store, or use student data. While I know the vast majority of us are using these data for good, the fact is the systems we have and are developing around these data can be used for the opposite. Relying on Congress to hold more hearings, or even pass new laws, is not enough. It is our responsibility, within our roles as parents and families, educators, administrators, researchers, and policymakers to balance availability with vigilance of our students' data. We need to educate ourselves about the rights and the responsibilities we have to protect students. Some of these responsibilities, like parents asking your school leaders how educational data are used and shared, or state policymakers establishing roles for data stewardship, are outlined at the previous links.

Educational data use is here to stay, and is in fact a potentially powerful tool in closing achievement gaps through truly equitable learning experiences. To benefit from this reality, rather than be hurt by it, let us step up and become better stewards of our students' data and their privacy. If we don't, Facebook has shown us how others could step in and take advantage.

.

Resources

Writing:

Ann Wylie – Rev Up Your Readership https://revvingupreadership.com/front/

Public Relations Society of the World – https://www.prsa.org/

Write like a journalist! - https://coschedule.com/blog/how-to-write-like-a-journalist/

Technical:

Symantic – https://www.symantec.com/blogs/

CISO Mag – https://www.cisomag.com/

Wired – https://wired.com

Brian Krebs - https://krebsonsecurity.com/