How To Cyber: *Submit Suspicious Emails*

Receiving junk emails, a.k.a. spam, is an inevitable fact of conducting business. Sending annoying quantities of unsolicited emails is primarily a commercial practice, but it is also a popular avenue for malicious attackers. These phishing attacks are extremely successful, because differentiating between normal and malicious emails is difficult. Especially when they can originate from known and unknown sources.

In order to combat phishing attacks campaigned against the Department, Cyber Security created the following simple and safe procedure to check suspicious emails:

Step 1: Save It

In Outlook: Navigate to *File > Save As*, and store the file locally on your workstation.

Step 2: Attach It

Create a new email and attach the file.

Step 3: Send It

Tell us why it is suspicious and send the email to Spam@dps.texas.gov. We will do the rest!

Suspicious Email Indicators:

◊ Abnormal spelling or sentence structure

◊ Strangely named attachments or file formats

◊ Asking for your personal information

◊ Anything requiring you to login or provide your password

If an email is **suspicious** in any way, please complete this procedure. Cyber Security never misses an opportunity to neutralize potential security threats. In fact, our analysts enjoy the challenge. For more information, read our step-by-step guide, or reach out to use directly at CyberSecurity@dps.texas.gov.

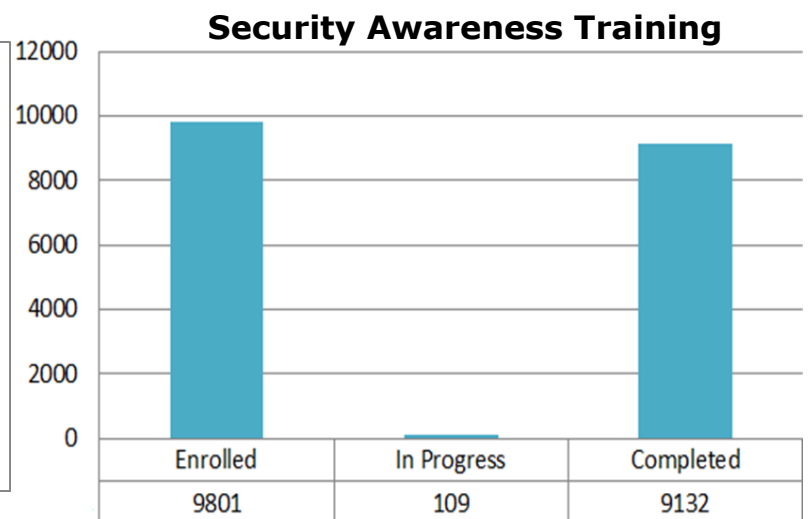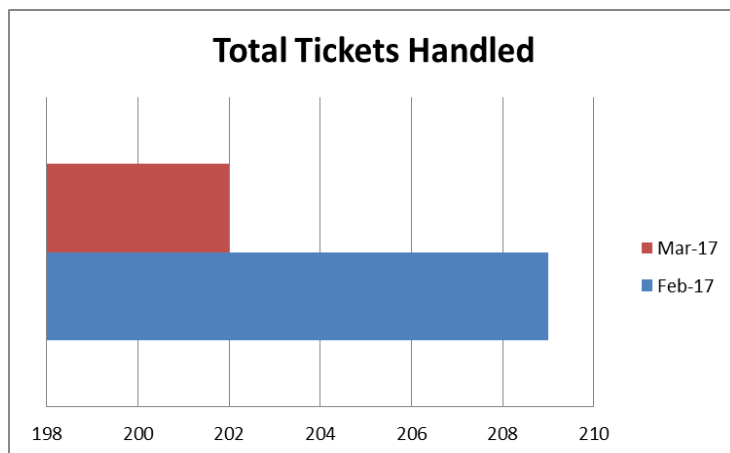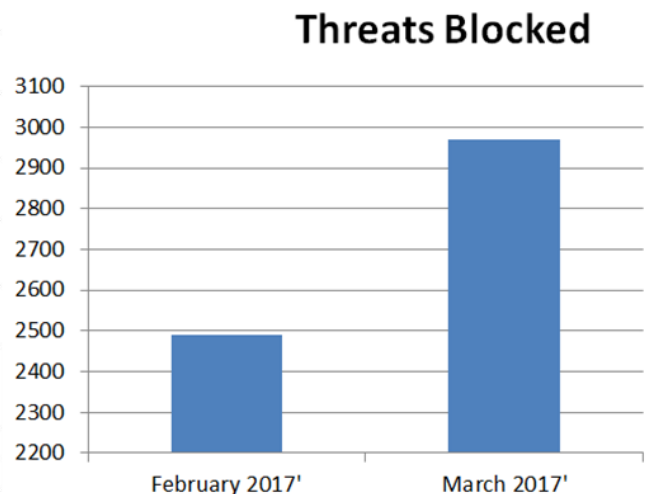Preventing phishing attacks is easy as pie...or
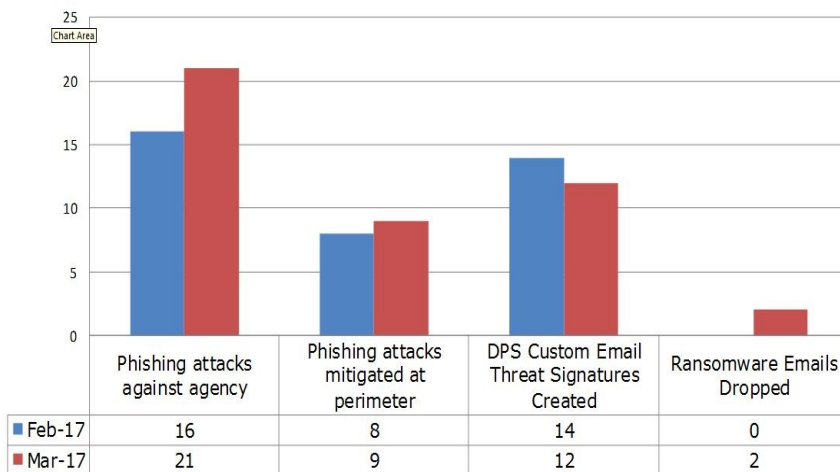
Whichever you prefer.

A Single Spear Phishing Click Caused the Yahoo Data Breach

A single click was all it took to launch one of the biggest data breaches ever. One mistaken click. That's all it took for a Canadian hacker aligned with rogue Russian FSB spies to gain access to Yahoo's network and potentially the email messages and private information of as many as 1.5 billion people.

The U.S. Federal Bureau of Investigation has been investigating the intrusion for two years, but it was only in late 2016 that the full scale of the hack became apparent. The FBI indicted four people for the attack, two of whom are rogue FSB spies who work for the division that is supposed to cooperate with America's FBI on cybercrime investigations. (The FSB is the successor of the KGB).
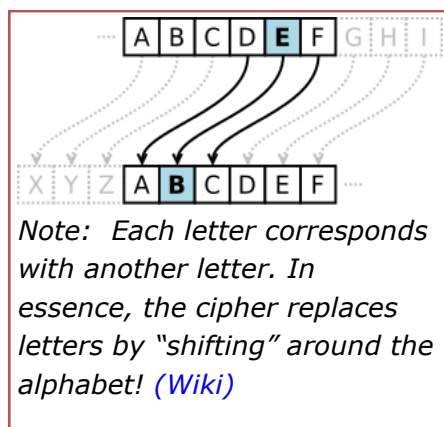
Read other relevant articles [here](#).

Cyber Security Stats: April 2017

	Phishing attacks against agency	Phishing attacks mitigated at perimeter	DPS Custom Email Threat Signatures Created	Ransomware Emails Dropped
Feb-17	16	8	14	0
Mar-17	21	9	12	2

Threats Blocked

(February 2017' — approximately 2490; March 2017' — approximately 2970)

Total Tickets Handled

(Mar-17; Feb-17; axis 198–210)

Security Awareness Training

Enrolled	In Progress	Completed
9801	109	9132

Crypto 101:
Showing the work

Sharpen your pencils, because *'Cyber-School'* is officially in session. Last month's challenge was a huge hit, and produced tons of great answers!

Note: Each letter corresponds with another letter. In essence, the cipher replaces letters by "shifting" around the alphabet! (Wiki)

For those who do not know, Crypto-Challenge 1.0 was a <u>Caesar cipher</u>. Named after Julius Caesar himself, this cipher is a basic encryption technique. It works by shifting letters of an alphabet against another alphabet. To keep it spicy for potential new readers, I will not provide the full solution; however, shifting the <u>alphabet 13 rotations</u> may be extremely helpful when decrypting last month's challenge.

Finally, kudos to all the readers and participants—especially our crypto challenge champions!

Crypto Challenge 2.0

"MDEwMDExMTAgMDExMDAxMDEgMDExMTAxMTAgMDExMDAxMDEgMDExMTAwMTAgMDAxMDAwMDAgMDEwMTAwMTEgMDExMDEwMDAgMDExMDAwMDEgMDExMTAwMTAgMDExMDAxMDEgMDAxMDAwMDAgMDEwMTEwMDEgMDExMDExMTEgMDExMTAxMDEgMDExMTAwMTAgMDAxMDAwMDAgMDEwMTAwMDAgMDExMDAwMDEgMDExMTAwMTEgMDExMTAwMTEgMDExMTAxMTEgMDExMDExMTEgMDExMTAwMTAgMDExMDAxMDAg"

Hint: *"This challenge is 64 times the fun"*

Email <u>Jennifer</u> your answer, or if you need help. Good Luck!