NEWS
Cyber Security
Vol. 2 | Issue 2
March 2017

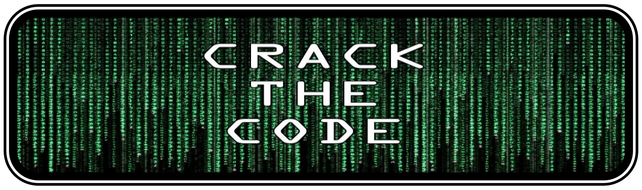
Ransomware | Crypto-Challenge | Spotlight | Passwords | Stats | IRS Alert

Ransomware Infection Causes Loss of 8 Years of Police Department Evidence

The Police Department in Cockrell Hill, Texas admitted in a press release that they lost 8 years' worth of evidence after the department's server was infected with ransomware. The lost evidence includes all body camera video, and sections of in-car video, in-house surveillance video, photographs, and all their Microsoft Office documents.

The press release says the infection took place after an officer opened a spam message from a spoofed email address imitating a department issued email address. New-school security awareness training would highly likely have prevented this.

Read full blog article here.



Do you have what it takes to be a security professional? The newsletter Crypto Challenge engages our audience, increases security awareness, and is super fun!

"Frphevgl njnerarff vf bhe funerq erfcbafvovyvgl."

Crack the encryption; tell Jennifer your answer; and get a shout out in the next newsletter.

Hint: *"Julius Caesar did good Cyber"*

Cyber Spotlight

Calling All Cyber Champions!

Work or personal life, share with us your best and most exciting cyber stories. From how you keep your software up-to-date; learned something new about security; or even derailed a targeted social engineering attack. We love hearing from our readers, and want to give credit where credit is due!

Thank you for working hard, and remaining vigilant.

Submit your stories to Jennifer anytime!

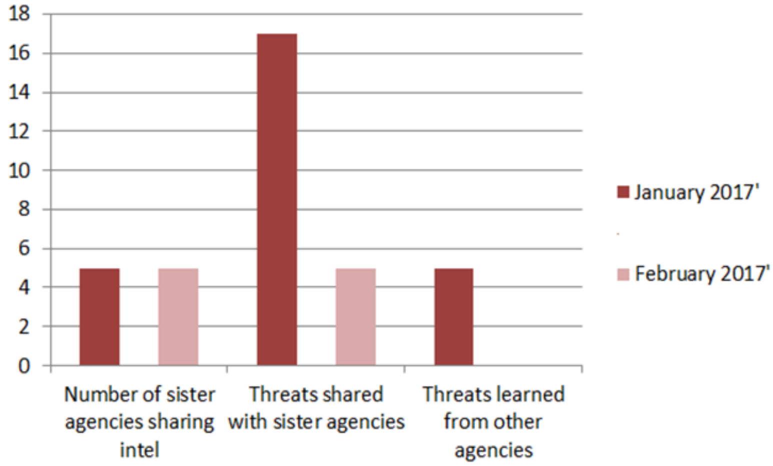
Choosing Secure Passwords

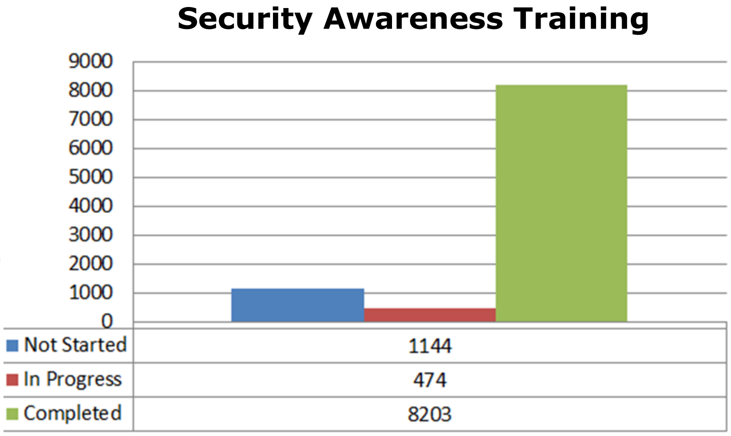
As insecure as passwords generally are, they're not going away anytime soon. Every year you have more and more passwords to deal with, and every year they get easier and easier to break. You need a strategy...

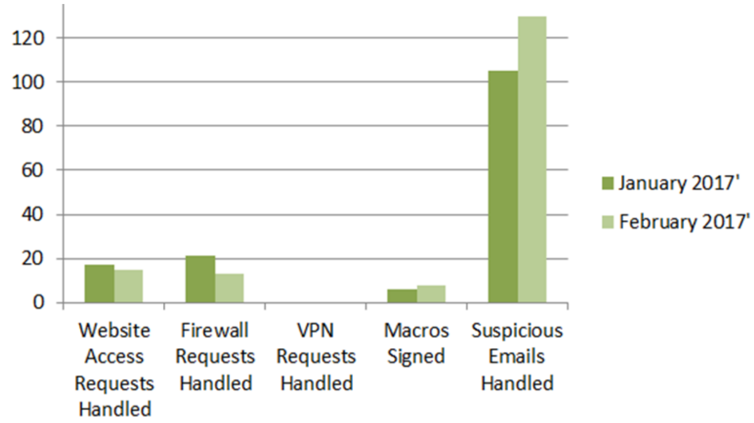
The efficiency of password cracking depends on two largely independent things: power and efficiency. **Power** is simply computing power. As computers have become faster, they're able to test more passwords per second; one program advertises eight million per second. These crackers might run for days, on many machines simultaneously. For a high-profile police case, they might run for months. **Efficiency** is the ability to guess passwords cleverly. It doesn't make sense to run through every eight-letter combination from "aaaaaaaa" to "zzzzzzzz" in order. That's 200 billion possible passwords, most of them very unlikely. Password crackers try the most common passwords first.

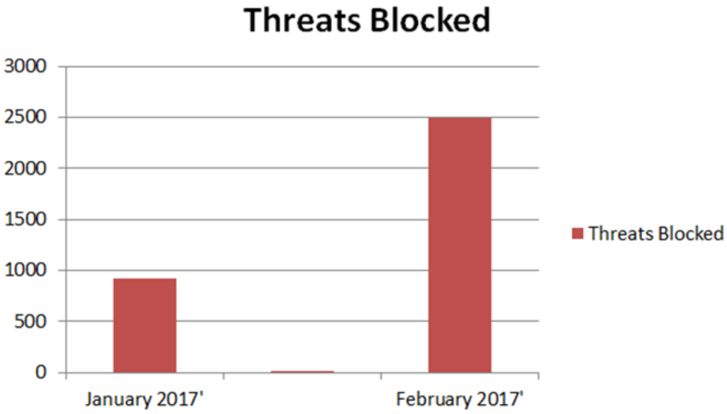
Learn to choose secure passwords by reading the full article here.

Cyber Security Stats: March 2017









ALERT

W-2 Phishing Scam

The Internal Revenue Service (IRS), state tax agencies and the tax industry issued an urgent alert to all employers that the Form W-2 email phishing scam has evolved beyond the corporate world and is spreading to other sectors, including school districts, tribal organizations and nonprofits. Read the Official IRS alert here.

The IRS will never:

- call to demand immediate payment using a specific payment method such as a prepaid debit card, gift card or wire transfer. Generally, the IRS will first mail you a bill if you owe any taxes

- threaten to immediately bring in local police or other law-enforcement groups to have you arrested for not paying

- demand that you pay taxes without giving you the opportunity to question or appeal the amount they say you owe

- ask for credit or debit card numbers over the phone

Tax season is here and online scammers are in full force. Learn how to best protect your and your family from scams by reading the IRS Security Awareness For Taxpayers.

Connect with us

For newsletter
support contact
Jennifer.Carson@dps.texas.gov

More Interesting Links

Slashdot
Security Week
Security Now

Visit the Website

Check out our Website for additional security information.