S.C.R.A.M. GAZETTE

FBI, Sheriff's Office warn of scam artists who take aim at lonely hearts

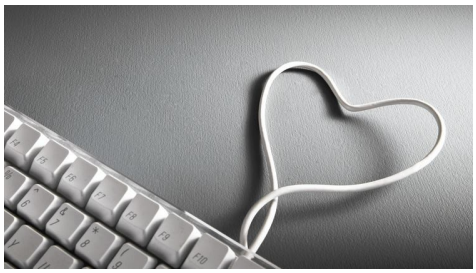
DOWNTOWN — The FBI is warning of "romance scams" that can cost victims thousands of dollars for Valentine's Day weekend.

A romance scam typically starts on a dating or social media website, said FBI spokesman Garrett Croon. A victim will talk to someone online for weeks or months and develop a relationship with them, and the other person sometimes even sends gifts like flowers.

The victim and the other person are never able to meet, with the scammer saying they live or work out of the country or canceling when plans are made, Croon said.

Then the scammer will say they need money, citing a sudden hardship like they need a visa or medical care, Croon said.

"And because you think you're in a relationship with this person, you wire the money to this person as it's directed overseas,"



Croon said.

Victims can be bilked for hundreds or thousands of dollars this way, and Croon said the most common victims are women who are 40 -60 years old who might be widowed, divorced or have a disability.

Romance scams cost people in Illinois more than $4.6 million in 2015. Nationally, the scams cost Americans $203 million.

"It's not uncommon to have someone to walk into FBI Chicago or into a field office in Illinois and report that they have sent thousands of dollars to someone they met online," Croon said. "And [they] have never even met that person, thinking they were in a relationship with that person."

If you meet someone online and it seems "too good to be true" and every effort you make to meet that person fails, "watch out," Croon warned. Scammers might send photos from magazines and claim the photo is of them, say they're in love with the victim or claim to be unable to meet because they're a U.S. citizen who is traveling or working out of the country, Croon said.

"Don't send money to this person," Croon said. "The chances of recovering your money are extremely slim."

If you have been scammed, you can go to IC3.gov and file a complaint, Croon said.
Source: **dnainfo.com**

AG Madigan Warns Of Immigration Scams After Executive Orders

CHICAGO — Illinois Attorney General Lisa Madigan is warning immigrant communities about potential scams in the wake of President Trump's recent executive orders on immigration.

Immigrants are cautioned to beware of scam artists or "unscrupulous immigration service providers" pretending to be lawyers or demanding excessive upfront fees, according to a statement from Madigan's office. They should also be cautious of people claiming to be law enforcement or government officials who demand money or threaten deportation.

Illinois law requires immigration service providers who are not licensed attorneys or nonprofits recognized by the Board of Immigration Appeals to register with Madigan's office. Legitimate immigration service providers must provide consumers with a written contract in English and their native language; provide a three-day right to cancel the contract; and return all documents to the consumer if requested, according to the AG's office.

Immigrants with concerns about traveling to their country of origin are encouraged to seek "reputable and legitimate" assistance and contact their local consulate.

"It is critical to find honest and legitimate assistance and know the warning signs of immigration fraud," Madigan said in the statement. "I encourage people to contact my office if you encounter a solicitation that seems questionable, or if you have already been the victim of fraud. My office does not ask for immigration status."

Complaints against immigration service providers can be filed by calling Madigan's office at (800) 386-5438, or her Spanish hotline at (866) 310-8398.

Source: CBS 2 Chicago News

Next Presentation
4/17 @ 11 AM
Home Repair Scams

Niles Police Department
7000 W. Touhy Ave
Niles, IL 60714
847-588-6500
www.nilespd.com

Connect with US!

WWW.NILESPD.COM

Security flaw reveals personal information at 3,400 websites

We always hear of cyber criminals causing havoc by breaking into web services with attempts to steal personal data. They can use various hacking methods like brute force, social engineering, zero-day exploits and software exploits and hacks.

But what if a simple typo in programming code could inadvertently leak out data without hacker intervention?

A coding error in a popular web optimization and content delivery company's programming was discovered to cause thousands of websites to leak sensitive data including passwords, encryption keys and cookies for months.

Affected sites include services like Yelp, OKCupid, Uber, Fitbit, ZipRecruiter, Patreon, Fiverr, Forbes, and 4Chan.

Cloudflare, whose service is used by more than 5.5 million websites, admitted in an official blog post that there was indeed a serious memory leak that may have contained sensitive information. The company said it has already identified and rectified the issue.

Google's Project Zero researcher and bug hunter Tavis Ormandy spotted the issue (unofficially nicknamed Cloudbleed) on February 18th and promptly informed Cloudflare about it.

(If you can recall, Ormandy is the same researcher who exposed flaws and bugs in popular software such as Symantec and LastPass.)

The Cloudflare leak was apparently caused by a single typo. By using the character – '>' rather than '=' – in Cloudflare's software source code, the vulnerability was created.

The greatest period of impact was from February 13 to 18, but the leakage may have been going on as far back as September 22 of 2016. Leaked sensitive data may have been cached by search engines which made this bug even more serious.

Cloudflare said the bug had been present in its code and unnoticed for years. A recent switch in its HTML parser changed how data is buffered, thus causing the memory leak.

To fix the problem, the company has turned off the three minor features (e-mail obfuscation, server-side excludes, and Automatic HTTPS Rewrites) that are causing the leaks, and claims the bug is no longer in effect.

Here's a list of some of the notable sites affected by "Cloudbleed":

- authy.com
- coinbase.com
- betterment.com
- fiverr.com
- transferwise.com
- prosper.com
- digitalocean.com
- patreon.com
- bitpay.com
- news.ycombinator.com
- producthunt.com
- medium.com
- 4chan.org
- yelp.com
- okcupid.com
- zendesk.com
- ziprecruiter.com
- uber.com
- poloniex.com
- localbitcoins.com
- kraken.com
- 23andme.com
- curse.com (and some other Curse sites like minecraftforum.net)
- counsyl.com
- tfl.gov.uk

Cloudflare asserts that there is no evidence of malicious exploits of the bug or signs of malicious use of the leaked information.

What you can do

Still, since the sensitive data has been potentially exposed for months and was cached publicly in search engines, it is wise to change your passwords if you are using any of the affected Cloudflare sites.

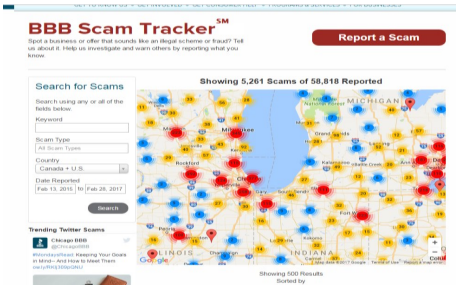
Also, it is a good idea to review your other passwords, Cloudflare site or not, since password reuse attacks will inevitably follow. With that said, it's a terrible practice to use the same username, email and password in multiple sites and services.

If the service offers it, it's also prudent to use multi-step verification or two-factor authentication if a service offers it. With this, a secondary code (for example, a code sent via text message to your phone) will be required to verify your identity.

Web services that are affected by this bug may also start sending out password change notices to their users, but please if you receive any, scrutinize them carefully since they might be phishing scams instead. Can you spot the signs of a fake email? Click here to take our quiz.

Source: ***www.komando.com***

BBB Scam Tracker



The Chicago Better Business Bureau has a great tool that can help you identify and report scams. You can then look at the scams as they are reported and see if they are trending or occurring in your area.

The website has an interactive map, as well as a table format that allows you to see the type, date and community that the scams occur.
https://www.bbb.org/scamtracker/us/

Internet Crime Complaint Center

The IC3 accepts online Internet crime complaints from either the actual victim or from a third party to the complainant. We can best process your complaint if we receive accurate and complete information from you. Therefore, we request you provide the following information when filing a complaint:

- Victim's name, address, telephone, and email
- Financial transaction information (e.g., account information, transaction date and amount, who received the money)

- Subject's name, address, telephone, email, website, and IP address
- Specific details on how you were victimized
- Email header(s)
- Any other relevant information you believe is necessary to support your complain

https://www.ic3.gov/default.aspx

2017 Events/Presentations

4/17 @ 11 am	**Home Repair Scams**
4/ 28— 9 am-2pm	**Mainestreamers Golf Mill Center**
5/17 @11 am	**Financial Exploitation**