

Cybercrimes (via cell phones) up in 2011

May 16 2012, By Claudia Buck

Addicted as we are to our online life and our mobile devices, it's no surprise that a growing number of cyber-criminals are lurking out there with us.

Their newest target is right in our hands: our cellphones.

Complaints of cyber <u>crime</u> topped 314,000 in 2011 - up 3.4 percent from the prior year - and California led the nation, according to a new report issued last week by the <u>Internet Crime Complaint Center</u>, a partnership of the FBI, the National White Collar Crime Center and the U.S. Department of Justice.

Online crime occurs in varied forms, from identity theft that uses personal information to commit fraud, to phony job schemes involving bad check deposits, to "romance scams" that seduce the lovelorn to send money to a pseudo-suitor. Nationwide, the average victim who filed a complaint last year was duped out of \$4,187, reported the center, known as IC3.

In the Sacramento region, the FBI's Dan Bryant said the most common scams are identity theft, advance-fee and non-delivery scams. For instance, victims can be defrauded on <u>Craiglist</u>, by <u>sending money</u> for items that never arrive or by applying for <u>job offers</u> that involve wire transfers of phony checks.

Cyber crime is thought to be a much larger problem than the numbers released Thursday suggest. Internet crime is "grossly under-reported"



nationally, said William Hinerman, IC3's unit chief. "We know there are tens of millions of computer users in United States and everybody who gets email, gets spam."

In announcing the annual Internet <u>crime statistics</u>, the center's deputy director Ken Brooks said he was "excited" by the increase in complaints - because it means more Americans are aware of online crime and realize they have somewhere to report it.

California, the nation's most populous state, posted the highest total number of Internet crime complaints last year, with 34,169. Next came Florida, then Texas, New York and Ohio.

On a per capita basis, however, the Golden State fared better: No. 13 in the nation. Based on complaints per 100,000 population, the states reporting the most fraud were Alaska, District of Columbia, New Jersey, Nevada and Colorado.

California ranked last when it came to reported losses per 100,000 population, at \$14.73. That compares with Washington, D.C., which ranked No. 1 with \$1,119.70 in losses per hundred thousand people.

While cyber crime has been around for years, the newest frontier for scam artists is mobile phones, the IC3 said.

And it's fertile territory. According to a recent Pew survey, about 83 percent of U.S. adults have a cell phone; of those, an estimated 42 percent have smartphones that can access email and the Internet.

Michael Parker, a retired rancher in Sacramento, has already seen cyberthieves sneak onto his T-Mobile cellphone. Last month, he had two text messages, purportedly from Wal-Mart, declaring he'd "won" a \$1,000 gift card. To claim his prize, he was instructed to click on a website.



Parker didn't take the bite. "Being a cynic helps," he said. "I'm not a Wal-Mart shopper, so that was one tipoff it was a scam."

Instead of clicking on the link, he called a local Wal-Mart manager to ask if the discount chain was giving out gift certificates by cellphone. The manager, Parker said, was "shocked, dismayed and not happy" to hear about the attempted scam, which likely was an attempt to install malware on his computer or trick him into giving out bank account or other financial information.

Parker also reported the phony texts to the sheriff's department and signed up his cellphone for the national "Do Not Call" registry, www.donotcall.gov.

Romance scams proved especially lucrative for scammers last year, according to IC3 statistics. At a rate of 15 complaints a day, these scams saw reported losses of roughly \$138,000, or more than \$5,700 every hour. The average victim's loss: \$8,900.

How to protect yourself from being swindled? The FBI's Bryant said individuals should "never give out any personal or financial information over the phone or Internet, unless he or she has personally initiated the communication."

Do your homework to verify the source of any online offers or official-sounding requests for your personal account information. In general, be skeptical of anything that sounds too good to be true.

For more details or to report a <u>cyber-crime</u>, go to: <u>www.ic3.gov</u>.

(c)2012 The Sacramento Bee (Sacramento, Calif.) Distributed by MCT Information Services



Citation: Cybercrimes (via cell phones) up in 2011 (2012, May 16) retrieved 11 May 2024 from https://phys.org/news/2012-05-cybercrimes-cell.html

This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.