

CRIME FIGHTER

The Safety Newsletter of the Oro Valley Police Department

Third Quarter 2016

Inside This Issue

Irish Smuggler 4

Scummer School 5

Contact
Information 9

CPTED: Natural Surveillance

As you may recall, in our last article of Crime Fighter we began discussing the different elements of CPTED – Crime Prevention Through Environmental Design. One of the things that I have always found fascinating about the whole premise of CPTED is this idea that we can have a practical impact on crime through something as simple as how we design and maintain our environments. Natural surveillance is a great balance of a lot of these ideas coming together in residential and commercial settings.

First, let me show you this picture of a Starbucks.



Seems like any Starbucks, right? But look closer, there's something going on along the right side of the photo that's worth pointing out:



As you can see, it's tables and chairs lined up against a glass window – with the windows open! There aren't graphics and advertising banners covering up the windows, there's not even shades in the way. This is a perfect example of using something like seating and tables to draw people to sit there, and by creating the openness of the windows this also creates a perfect opportunity for people to be looking out the window in to the parking lot.

One of the things that businesses have a hard

Oro Valley
POLICE

www.ovpd.org

CPTED: Natural Surveillance Continued

time with occasionally is property crimes occurring in the parking lot. When you have a big concrete wall facing out in to the parking lot, it can some times create an environment that's perfect for criminals to break in to vehicles and commit other crimes.

Here's an example of a parking lot with very little natural surveillance observed:



Concrete walls and no one around in sight. This is not inviting!

Other examples of this include the window bars that various restaurants utilize, like this picture:



This is another great example of how TO do natural surveillance.

CPTED: Natural Surveillance Continued

While these examples are focused on commercial settings, a similar idea can be approached within the suburban and residential areas as well.



Here's an example of things being done wrong. The trees and bushes have been ignored so long that they're covering the windows, obstructing the view out the street to the front of the house.

An example of CPTED being done well can be seen here:



What's great about this is the line of bushes around the bottom of the windows are kept well below the windows, and the trees are kept trimmed high enough to allow for a person to see out the street without issue.

Just remember, the overall goal of natural surveillance is to maximize the surveillance ability for you to see out and survey the environment for what's going on!

Irish Smuggler



As you may recall in our last edition of Crime Fighter, we had an article in there from DHS regarding elderly being duped in to smuggling:

After that I ran across a fascinating story out of Ireland about a retired surgeon from Florida who had been duped in to smuggling Cocaine in to Ireland.

<http://www.thesun.ie/irishsol/homepage/news/7117542/Top-doctor-pleads-guilty-to-smuggling-100k-worth-of-cocaine-into-Ireland.html>

A TOP US surgeon fell victim to a scam which led him to smuggle €100,000 in cocaine through Dublin Airport, a court heard.

Dr Carlos Cruz Soriano, 76, from Florida, who has early onset dementia, began responding to phishing emails after becoming isolated and depressed following his retirement from a “glittering career”, Dublin Circuit Criminal Court was told.

The scammers told him a long lost relative had left him €2 million in a will.

They gained Soriano’s trust before flying him to Colombia where he was given the papers for his inheritance as well as a “gift” in a bag for Irish bank officials who would facilitate the cash transfer.

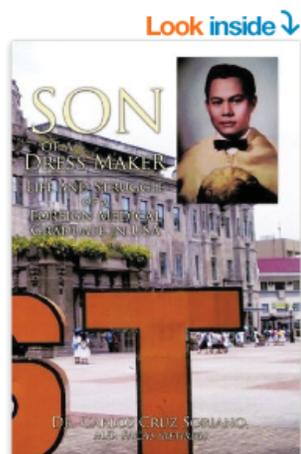
Soriano pleaded guilty to possession of cocaine valued at €107,000 in the arrivals hall at Dublin Airport on September 1, 2015.

He has no previous convictions and has been in custody here since his arrest.

Judge Melanie Greally indicated that she would impose a five-year sentence which she would fully suspend on condition he leave the country. She adjourned the case until next week.

This was absolutely heartbreaking to read. I was left with many questions like, how could one go from being a surgeon, holding peoples’ lives in your hands, to falling for some fake emails?

Digging in to this story a little more I discovered that this doctor was also a published author whose book you can buy on Amazon.



Look inside ↓

Son of a Dress Maker: Life and Struggle of a Foreign Medical Graduate in USA

Paperback – February 11, 2011

by Dr Carlos Cruz Soriano M. D. Facas (Author)

Be the first to review this item

▶ See all 3 formats and editions

Kindle
\$8.69

Paperback
\$14.03

Read with Our **Free App**

3 Used from \$15.28
11 New from \$11.82

My struggle in life from my childhood, formative years and my schooling from primary grades, high school and college of medicine. My determination to succeed in life to the pinnacle of my profession.

This is a heart-breaking and tragic case that serves as a potent reminder of the dangers that deteriorating mental health can pose. Here’s a surgeon who’s also a published author that has been conned in to becoming a drug mule, and is now in a foreign prison as a result.

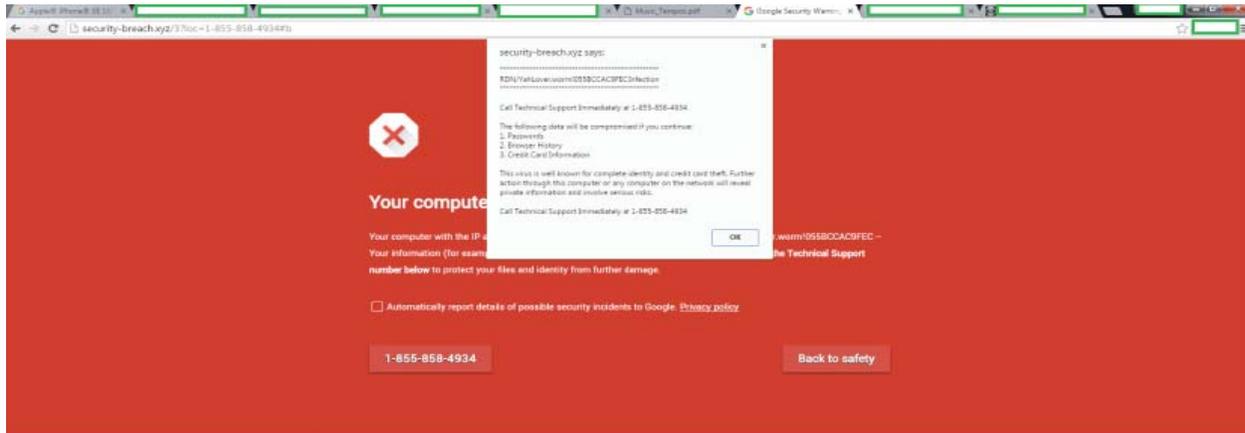
Let’s take care of our friends and family and make sure we don’t see more headlines like this.



See this image

Scummer School

It's summer, we're in Tucson, and we've been having a lot of fun at our Scam School events talking about Identity Theft and other incidents. Recently there's been a rising wave of issues involving the "Tech Support" and "computer virus" scams. This just happened to me at home last night! Here's a screenshot of what I saw:



To give you some background, I was looking for some information on an upcoming trip where I would be bagpiping. When I visited one site, I was redirected to this big scary looking red screen that told me I had a security breach, and it was directing me to call a 1-800 number. My screen was frozen and I couldn't click the "x" icon to close anything. Some other tricks I tried:



Holding down on the "windows" key and the "D" key at the same time did successfully automatically take me to my desktop and minimize all other windows.

Trying to right-click on the "Chrome" icon and click "close windows" did not work.

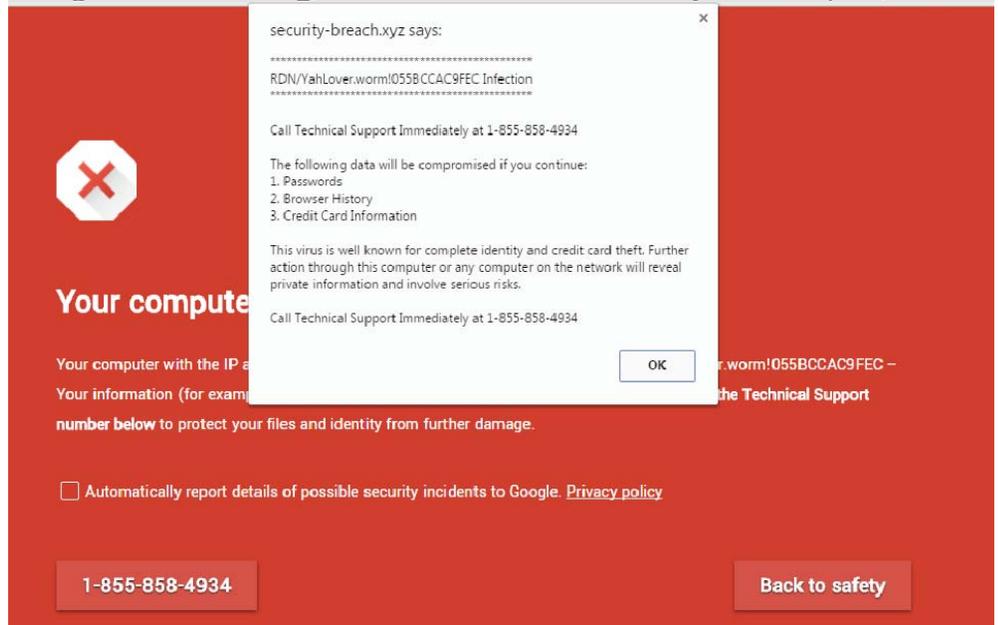
Finally, I held down on the "alt" and "F4" keys at the same time, and that successfully closed the browser and all the windows (including the

stuff I was working on). (Go ahead and try that right now – **warning**, it will close whatever window you have open.)

Of course I took some screenshots because when people are trying to hack you, it's fun to take pictures along the way!

So let's take a look at some of the elements of this little scam and unpack it to find the truth of what's going on.

Does Google give you 1-800 numbers to call if you've been hacked? No. They do not.



Scummer School Continued

That's how I knew right off the bat that this was a scam, although the logo on the browser tab is the same as the one for Google, and it even says "Google Security Warning".



855 area code



All Shopping Maps News Apps More Search tools

About 1,370,000 results (0.37 seconds)

Area code 855 is a non-geographic area code, meaning that it is not associated with any particular city, state, province, or country. Area code 855 is a toll free number, that recently joined the list of 800, 888, 877, 866, and 844 toll-free numbers. Possibly Cambodia.

Additionally, when I researched that number I found that the 855 area code is associated with Cambodia. Not exactly something that comes to mind when you think of Google tech support.

I then took a look at the website address in the browser bar – it had nothing to do with google.com. In fact, it was security-breach.xyz.

Now this is very odd. If you're not familiar with domains, that's everything between the last "." in a website's name and the first "/". In this case, the top-level domain is ".xyz" instead of ".com" or ".org" like we're used to seeing.



What many people don't know is that you can actually look up a website to see where it's being hosted and where it's from. While the top-level domain for that particular site is ".xyz" the domain itself is "security-breach.xyz" and we can run that like a car's license plate to see who owns it. In this case, we find out some interesting information, but not much. Firms offer services to protect the identity of the real owners of various websites. The owners can be located by looking up the "whois" information. Here's what we find for security-breach.xyz

Whois record for security-breach.xyz

```
Domain Name: SECURITY-BREACH.XYZ
Domain ID: D14987467-CNIC
WHOIS Server: whois.namecheap.com
Referral URL:
Updated Date: 2016-02-24T10:17:32.0Z
Creation Date: 2016-02-03T16:05:40.0Z
Registry Expiry Date: 2017-02-03T23:59:59.0Z
Sponsoring Registrar: Namecheap
Sponsoring Registrar IANA ID: 1068
Domain Status: clientTransferProhibited
```

From here we find something interesting that I point out with the blue box – this was created February 3rd of 2016. This is a relatively new website! Very common with someone trying to run a scam since they constantly have to create new websites when their old ones get noticed and taken down.

From there I used a website called network-tools.com and I ran a trace. This is what I found:

The number at the top, 51.254.45.97, is called the Internet Protocol, or IP address. Humans find it easier to remember names like "google.com" and "security-breach.xyz" but your computer knows those websites by their IP addresses.

When we run a trace like this we see every hop your computer takes to visit this site. It landed at a place called sharkserve.rs. Sharkserve.rs is a company that hosts websites, and .rs is the country domain for Serbia (Republika Srbija).

51.254.45.97 is from Other (XX) in region Unclassified
Input: security-breach.xyz
canonical name: security-breach.xyz
Registered Domain: security-breach.xyz

TraceRoute from Network-Tools.com to 51.254.45.97 [security-breach.xyz]

Hop	(ms)	(ms)	(ms)	IP Address	Host name
1	0	0	0	206.123.64.233	-
2	36	0	0	206.123.64.45	-
3	1	0	0	64.124.196.225	xe-4-2-0.er2.dfw2.us.above.net
4	1	1	1	64.125.29.121	ae8.er1.dfw2.us.zip.zayo.com
5	1	1	1	64.125.20.65	ae11.cr1.dfw2.us.zip.zayo.com
6	103	104	132	64.125.30.180	ae27.cs1.dfw2.us.eth.zayo.com
7	146	108	104	64.125.28.98	ae5.cs1.iah1.us.eth.zayo.com
8	104	104	104	64.125.29.48	ae3.cs1.dca2.us.eth.zayo.com
9	128	104	104	64.125.29.130	ae5.cs1.lhr15.uk.eth.zayo.com
10	107	107	108	64.125.30.235	ae27.mpr3.lhr3.uk.zip.zayo.com
11	104	105	104	64.125.21.22	ae6.mpr2.lhr3.uk.zip.zayo.com
12	Timed out	Timed out	Timed out		-
13	108	111	108	91.121.128.86	be11-1187.rbx-g1-a9.fr.eu
14	Timed out	Timed out	Timed out		-
15	108	107	108	51.254.45.97	aurora.sharkserve.rs

Trace complete

Scummer School Continued

So let's review what we have here:

- An alleged Google website telling us to call a 1-855 number (that's odd – I can't remember Google ever giving me a contact number before)
- The 1-855 area code comes back to Cambodia
- The website, security-breach.xyz, is relatively new (created in February of this year – Google is a lot older than that)
- It's hosted in Serbia (Enough said?)

Overall, everything about this is odd.

Next Steps

The way this scam is supposed work is they want you to call the 1-855 number at which point you will be put in touch with "tech support." They may even make you sit on hold like they're really a busy tech support department!

They will then walk you through a number of semi-complicated steps and get you to download something on to your computer that will give them remote control of it. You will sit back and watch in horror as they move the mouse across your screen and steal your passwords, your bank account information, and anything else you access from your computer. They will then ask you for your credit number so they can charge you around \$500-\$700 to "fix" your computer.

Yes, they have the audacity to charge you a fee while stealing your sensitive information. The nerve...

Fixing the hack

From here you will need to go find a traditional computer repair company, one that you can visit in-person here in town. They are quite familiar with these scams and will know how to handle cleaning up your computer.

And finally, change your passwords! For everything! Chances are the bad guys probably have a copy of your passwords for your banking, investments, and even email. Changing those passwords will prevent them from having continued access to your accounts.

IRS Warns of Latest Scam Variation Involving Bogus “Federal Student Tax”

WASHINGTON — The Internal Revenue Service today issued a warning to taxpayers about bogus phone calls from IRS impersonators demanding payment for a non-existent tax, the “Federal Student Tax.”

Even though the tax deadline has come and gone, scammers continue to use varied strategies to trick people, in this case students. In this newest twist, they try to convince people to wire money immediately to the scammer. If the victim does not fall quickly enough for this fake “federal student tax”, the scammer threatens to report the student to the police.

“These scams and schemes continue to evolve nationwide, and now they’re trying to trick students,” said IRS Commissioner John Koskinen. “Taxpayers should remain vigilant and not fall prey to these aggressive calls demanding immediate payment of a tax supposedly owed.”

Scam artists frequently masquerade as being from the IRS, a tax company and sometimes even a state revenue department. Many scammers use threats to intimidate and bully people into paying a tax bill. They may even threaten to arrest, deport or revoke the driver’s license of their victim if they don’t get the money.

Some examples of the varied tactics seen this year are:

- Demanding immediate tax payment for taxes owed on an iTunes gift card.
- Soliciting W-2 information from payroll and human resources professionals—IR-2016-34
- “Verifying” tax return information over the phone—IR-2016-40
- Pretending to be from the tax preparation industry—IR-2016-28

The IRS urges taxpayers to stay vigilant against these calls and to know the telltale signs of a scam demanding payment.

The IRS Will Never:

- Call to demand immediate payment over the phone, nor will the agency call about taxes owed without first having mailed you a bill.
- 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.
- Require you to use a specific payment method for your taxes, such as a prepaid debit card.
- Ask for credit or debit card numbers over the phone.

If you get a phone call from someone claiming to be from the IRS and asking for money and you don’t owe taxes, here’s what you should do:

- Do not give out any information. Hang up immediately.
- Contact TIGTA to report the call. Use their “IRS Impersonation Scam Reporting” web page or call 800-366-4484.
- Report it to the Federal Trade Commission by visiting FTC.gov and clicking on “File a Consumer Complaint.” Please add “IRS Telephone Scam” in the notes.
- If you think you might owe taxes, call the IRS directly at 1-800-829-1040.

More information on how to report phishing or phone scams is available on IRS.gov.



Dispose-A-Med Oro Valley

Clean out your medicine cabinets

Bring your unused or expired prescription and over the counter medications and we will dispose of them for you properly. We accept pills and liquids.

This includes veterinarian medications and vitamins. Please keep all pills in their original containers. Bins will be provided for you to drop off your medications and it is completely anonymous. Please do NOT bring batteries or household hazardous waste.

Upcoming prescription-take-back events in 2016:

Target 10555 N. Oracle Road 10 am - 2 pm	Walmart 7951 N. Oracle Road 10 am - 2 pm	Sun City Oro Valley 1495 E. Rancho Vistoso 9 - 11 am
02/06/16	04/02/16	03/08/16
08/06/16	06/04/16	09/13/16
10/16/16	12/03/16	11/08/16



We will no longer be accepting metal or glass inhalation aerosol containers, syringes or epi-pens. For your convenience, the following is a list of companies that offer mail back disposal kits for a fee:

Target Pharmacy Department	Total Home Medical www.totalhomemedical.com	Stericycle www.stericycle.com	Republic Services www.republicsharps.com
--------------------------------------	---	---	--



For more information contact the OVPD Community Resource Unit, at (520) 229-5080

Mark Your Calendar

Fourth of July - James Kriegh Park
July 4

Dispose-A-Med Target
August 6 10 am - 2 pm

Sun City Oro Valley - 1495 E. Rancho Vistoso
September 13 9 - 11 am

National Night Out
October 7 6 - 8 pm



Fun facts about Oro Valley

Q: Who were the two immigrants that set up Steam Pump Ranch?

A: George Pusch and Johann Zellweger

Q: Steam Pump Ranch sits by what major watershed?

A: Canada Del Oro

Q: Where in Oro Valley can you see these amazing petroglyphs?



A: Honey Bee Canyon

**Oro Valley
POLICE**
www.ovpd.org

Contact Information

OVPD Crime Prevention Unit
Northside Substation
1171 E. Rancho Vistoso Blvd., Suite 115
Oro Valley, AZ 85755
(520) 229-5080
(520) 229-5090 fax

Office Hours
Monday – Friday
8 a.m. – 5 p.m.

Sgt. Amy Graham
(520) 229-5081
agraham@orovalleyaz.gov

Ofc. Elijah Woodward
(520) 229-5085
ewoodward@orovalleyaz.gov

Ofc. Marshall Morris
(520) 229-5084
mmorris@orovalleyaz.gov

Like us on Facebook: www.facebook.com/OroValleyPoliceDepartment

Like the Chief on Facebook: www.facebook.com/ChiefSharp

Follow us on Twitter: www.twitter.com/OroValleyPD

**Add our Android or iPhone App, MyPD
available in the Android Market or App Store.**

