



MIGNOLET
BUSINESS RESEARCH CONSULTANTS, INC.

Drugs in the Deep Dark Web
Cyber Thieves in CEO Clothing



CE/CLE Training

Jean Mignolet is proud to offer CLE approved trainings regarding tips for "Locating Hidden Assets" and "Google is not an Investigation" for legal professionals and attorneys. Please contact for available dates.

For more than three decades Jean Mignolet has served in law enforcement and private investigation, managing all aspects of general investigative business. She specializes in in-depth background investigations, and is the top choice of attorneys, corporations, small business owners and individuals who require all types of investigative services.

For further information visit: www.Mignolet.com

Dear Debbie,

In this day and age, you can do nearly everything over the internet. You can buy goods and listen to music from around the world, conduct business, transfer money, and keep in touch with coworkers and friends via email and social media.

You can also scam businesses for millions of dollars by stealing client lists. Individuals can buy any narcotic you could possibly imagine on the dark web.

This month, we take a look at just how far our interconnection with the internet goes - from the massive unseen world of the dark web to cleverly crafted scams made possible by business webpages and social media profiles.

Our lives online are not going away. Protecting ourselves and our businesses is possible and preferable to privacy violations to justify keeping us safe. Staying safe is a DIY project!

Jean Mignolet

Contact us at:
Mignolet@Bellsouth.net
or call us at: 954-523-8737 or
954-336-9363

Quick Links
[Our Website](#)

[Services](#)

Join Our Mailing List!

Drugs in the Deep Dark Web

Just how big is the Dark Web drug trade? Big enough for police in Leipzig to raid 38 locations, confiscate more than a third of a ton of various narcotics, and barely make a dent.

The dark web drug market known as **Evolution is a top drug market on the dark web.** It is a hub for online drug operations worldwide. In this particular bust, police in Germany - which clocked in at the largest bust of its kind to ever happen in the country - took down an operation that utilizes the Evolution drug market to sell everything from cocaine and methamphetamine to LSD and ecstasy.

This particular operation that utilized Evolution to reach its client base is known only to customers as "Shiny-Flakes." This international drug

A reminder that prior issues of the newsletter are viewable from the website.

Cyber Thieves in CEO Clothing

The FBI reported that hijacked email accounts were responsible for businesses losing nearly \$215 million to cyber thieves in the past 14 months. These crimes start with the hijacking of an email account of a company's executives or employees and businesses who commonly perform wire transfers or deal with



suppliers from overseas are especially at risk. No business is safe from this

scam, and these particular cons are becoming evermore nuanced to the inner-workings of the businesses they target.

Since staff information is readily available on company websites, along with calendars, and travel plans - not to mention all of this is augmented by what people disclose about their lives and their schedules on social media - it has become easier for scammers to glean details about the people who they pose as. They can also pick up on how to write in the tone of the business and its employees to make fraudulent emails feel more compelling and camouflaged from suspicion.

In a common permutation of this scam, the con artist poses as a company's executive and sends a request to the employee who typically handles wire transfers

trafficking organization is allegedly run by a 20-year-old man living in Leipzig who was arrested in the bust, alongside a 51-year-old Bulgarian man who is suspected to be the courier who moves drugs from the operation's supplier based in Holland. The bust raided 38 locations of operation for this single organization. Almost one third of a ton of narcotics were seized in the raids alone, which doesn't count the 100 pounds police bought from the group themselves as part of the sting. All told, police came into possession of around \$4.25 million in narcotics from Shiny-Flakes.

\$4.25 million is hardly a significant number in the grand scheme of the online drug trade on the dark web. The magnitude of what is going on in the darkness of the world wide web is almost incomprehensible.

To learn more about the Dark Web, the blog www.deepdotweb.com keeps an eye on what's going on down there in the dark, or at least the parts that come to the surface.

to wire money. Little details can be dropped about travel dates, meeting times, and even family members to lead the recipients of these emails to believe it's just business as usual, especially if being asked to wire money is a normal workplace occurrence.

The Internet Crime Complaint Center (a collaboration of the FBI and the National White Collar Crime Center) explains:

"The requests for wire transfers are well-worded, specific to the business being victimized, and do not raise suspicions to the legitimacy of the request. [...] Fraudulent emails received have coincided with business travel dates for executives whose mails were spoofed. The subjects are able to accurately identify the individuals and protocol necessary to perform wire transfers within a specific business environment."

Talk about a clever disguise!

How can businesses protect themselves against such complex and compelling scams? The Internet Crime Complaint Center advises a two-step authentication process for emails, and also to include other channels of communication regarding wire transfers to verify transactions before they are submitted. This way, employees can't just wire money when prompted via email, even if the email is from a legitimate source.

Another precautionary step advised is to encourage businesses to limit the amount of employee activity information made available both on the company website and on social media.

