The Dark Web has your online identity for sale - Here's how to protect yourself

By Francis Navarro, Komando.com, March 30, 2018

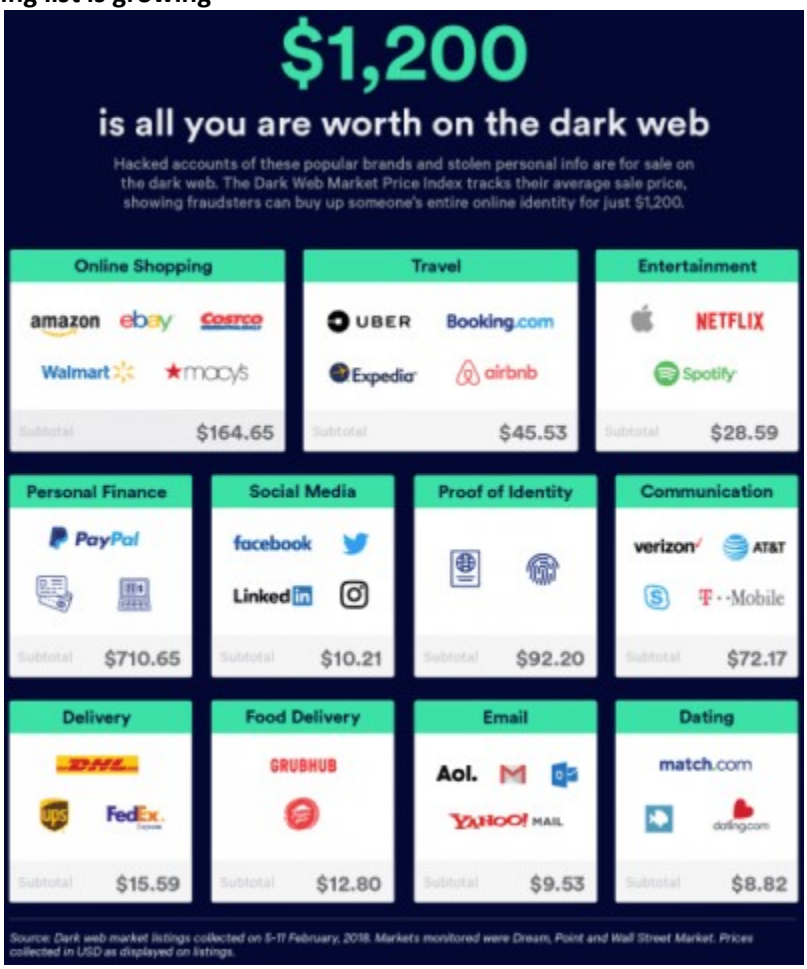
Recently, we told you about how your entire online identity is up for grabs on the Dark Web for cheap.

The assortment of stolen data that was discovered is sobering - Netflix, Uber, Spotify and Airbnb logins (all yours for the low price of $10 each), email accounts like Gmail and Yahoo (as low as $1) and social media accounts (around $2 each). The high ticket items seem to be personal finance information like PayPal and credit card data. Asking price? Around $250 each.

And check this out, for ultimate savings, cybercriminals also sell entire packages (known on the Dark Web as "fullz") filled with vital sensitive information like your name, billing address, mother's maiden name, Social Security number, date of birth and other personal data.

That's more than enough to do irreparable damage to anyone's life!

The cybercriminal's shopping list is growing



Based on the average prices of each kind of stolen account that are for sale on the Dark Web, if someone is going to purchase all the available items for a single person, the checkout price is just $1,170. Yep, one person's entire online identity is cheaper than a refurbished MacBook Pro.

It's such a lucrative Dark Web trade that stolen data outfits are adopting legitimate marketing practices. Buying a set of multiple "fullz" is cheaper and I won't be surprised if they started selling specific bundles soon.

Want to save? Do an entertainment bundle (Netflix, iTunes, Spotify)! How about an online shopping bundle (Amazon, eBay, Walmart, Costco) with free shipping! Maybe they'll start having Dark Friday sales too. It's a scary thought but it's just a matter of time.

How do you stop this smorgasbord of data?

Sadly, your data may already be floating on the Dark Web without you knowing it. There's a website called HaveIBeenPwned that tracks emails and usernames that are known to have been stolen in data

breaches. Run your email through the site's search and it will alert you your email and associated accounts are already out there.

Keep changing your account passwords regularly and always create strong ones to replace your old ones. Never ever reuse your passwords or have the same password for different accounts. We recommend having a good password manager like RoboForm. Whenever available, turn on two-factor authentication for an extra layer of protection.

Constantly check your accounts for unauthorized activity - movies on your Netflix profile that you don't remember streaming, mystery purchases that you haven't made, songs on your Spotify that you didn't listen to, credit card charges that came from nowhere - if something's amiss, report it immediately.

If you think you are already compromised, put a credit freeze on your accounts as soon as you can.

How do you prevent your data from being stolen in the first place?

Well, phishing is still the most popular method hackers are using to steal personal information. Beware of sketchy emails with unknown links and never ever click on attachments. Be vigilant even against legitimate-looking emails, always check the URLs and always go to a service's official site to log in.

Also, don't let your unused accounts go stagnant. Track down any old accounts that you no longer need and close them all out.