## The Hidden Economy: Dark Web and Encrypted Marketplaces

by The ThreatAdvice Faud Team

Within the internet lies a hidden layer called the dark web which requires specific methods for access. Within this hidden realm, dark web marketplaces operate as platforms for various illicit activities. However, there are also encrypted marketplaces offering illegal activities on platforms such as Facebook or Telegram. It is crucial to understand these marketplaces, their unique characteristics, and the dangers they pose particularly for vulnerable financial institutions.

**Understanding the Dark Web**

The internet is commonly divided into three parts:

1. **Surface Web:**This part includes what you use every day on the internet. It's accessible through standard web browsers. Example: [**google.com**](https://nam10.safelinks.protection.outlook.com/?url=http%3A%2F%2Fwww.google.com%2F&data=05%7C02%7Cjtaer%40threatadvice.com%7Cc5513f5066b54442a99d08dc8bd57ecf%7C375b7f7ba1f54671a3419b30a7e614da%7C0%7C0%7C638538996289575822%7CUnknown%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3D%7C0%7C%7C%7C&sdata=2%2FnZGUjyeDKtMqngy2WuxKSwa1Tcur1H2JhENCYXZy8%3D&reserved=0).
2. **Deep Web:**This includes all web pages that aren't discoverable on search engines. Example: Email inbox or private databases.
3. **Dark Web:**This is a smaller and hidden part of the deep web. It needs special tools to access it like Tor (a web browser). It's purposefully hidden and used for anonymity. Example: The black market.

Dark web marketplaces are online platforms where users trade illegal goods and services. They operate like regular online stores but sell illicit items, such as drugs, weapons, personal data, counterfeit goods, and illegal services like hacking or hitmen for hire. An example is shown in *Figure 1.*



*Figure 1: A dark web marketplace selling or giving out private information from different institutions, including financial.*

**What Are Encrypted Marketplaces?**

Encrypted marketplaces are online platforms that utilize robust encryption to maintain user privacy while enabling the buying and selling of goods and services. Unlike traditional online stores, these platforms often facilitate transactions involving illegal items and services, and they can be accessed through popular platforms like Facebook or Telegram making them easier to enter and use compared to dark web marketplaces. They include similar illicit goods and services offered at dark web marketplaces. An example is shown in *Figure 2*.



*Figure 2: The left image shows a Telegram group selling stolen checks. The right image shows a group on Facebook selling bank loads and CVV deals.*

**How Are Dark Web Marketplaces Different from Encrypted Marketplaces?**

While both dark web and encrypted marketplaces use encryption to protect user privacy, their purposes and operations are distinct:

1. **Dark Web Marketplaces:**
	* **Specialized Software:**Require special tools like Tor to access, making them more hidden and anonymous.
	* **User Base:**Frequented by criminals looking to buy or sell illegal goods and services anonymously. It is harder to find and access these services.
2. **Encrypted Marketplaces:**
	* **Legitimate Platforms:**Use end-to-end encryption to ensure privacy and security for users, often found on mainstream apps like Facebook and Telegram.
	* **User Base:**Often used by criminals looking to buy or sell illegal goods and services to the common person. Users can access these services trouble-free.

The dark web is accessed by experienced internet users, unlike encrypted marketplaces. Since encrypted marketplaces are more accessible to the average person, this accessibility can lead to real-world consequences, affecting users on mainstream platforms unknowingly.

**The Impact on Financial Institutions**

Illegal activities on encrypted marketplaces can have significant impacts on financial institutions:

* **Fraudulent Transactions:**Stolen banking information and personal identities are frequently traded, making financial institutions prime targets for fraud.
* **Security Breaches:**Hackers can purchase malware and other tools to launch attacks, leading to data breaches and financial losses.
* **Reputational Damage:**Incidents of fraud and breaches can significantly harm the reputation of financial institutions, eroding customer trust and loyalty.

**Maintaining Online Safety**

Understanding these marketplaces highlights the importance of being cautious online. Here are some tips for smaller institutions to protect themselves:

* Invest in [**strong cybersecurity framework,**](https://www.threatadvice.com/mssp?__hstc=244925338.67aa4bfeb74326f15d3875b003849e58.1725029908284.1727281987700.1727384945473.15&__hssc=244925338.11.1727384945473&__hsfp=4134642422) including firewalls and encryption.
* Regularly train staff on the latest cybersecurity threats and best practices for preventing fraud and data breaches.
* Implement systems to detect unusual transactions or access patterns that could indicate a breach.
* Collaborate with local authorities to stay informed about current and emerging threats.

At ThreatAdvice we provide innovative fraud prevention solutions **[TAFraudSentry](https://www.darkdefend.com/fraudsentry%22%20%5Ct%20%22_blank)** and **[FraudXchange](https://www.darkdefend.com/fraudxchange%22%20%5Ct%20%22_blank)** designed to help banks and credit unions detect and stop check fraud before it causes significant damage. Our tools monitor account activity in real time, ensuring your institution is protected from various type of fraud.

If you're interested in learning more about how our solutions can safeguard your business, [**contact us**](https://www.darkdefend.com/contact)today or explore our range of fraud detection services.