The Dark Side of the Web

Remember the heydays of the late 1990's? You know, the .com bubble? Those were days that will never be forgotten. The major financial indices here in the United States and around the world hit all-time highs, and everybody was making a lot of money. Any business with a .com in its name was basically receiving unlimited funding from Venture Capitalists.

Nobody questioned about seeing a business plan, as long as you had something or another on the Internet, you got funded. But of course, all good things must come to an end, and so did the .com bubble, by 2000. No longer was .com the norm, and to receive any investor money, you now had to have a rock solid business plan.

But despite the economic losses we saw with the .com bubble as it burst, there are few things it has left behind which are still predominant today on the Web. Probably its biggest legacy is that of E-Commerce. During this time, a lot .com businesses were trying to sell their respective products and services on the Web. But, many of the online shopping carts at this time were still evolving, and did not possess the functionality we see today.

In these modern times, we are able to shop literally anywhere at any time as long as we have an Internet connection. There is no more need to visit a brick and mortar store anymore, we can select what we want from the convenience and comfort of our Smartphone, and within minutes, make the payment as we choose fit, as well as the shipping method.

But despite all of the advantages that the Web has brought with this revolutionary shopping experience, it has also been accompanied with a negative flip side. That is, the it has now become the prime target for Cyber based attacks. On an almost daily basis, there is a sophisticated and covert attack which has been launched in order to bring down an E-Commerce site, and anything else associated with it.

For example, usernames and passwords can be stolen, as well as credit card information. If a customer becomes a victim, these are just the mere short term impacts. There will more than likely will also become a victim of Identity Theft, which could take years to rectify. Not only that, but Cyber Attackers are now luring customers to fake websites which look like original, authentic ones. The damage only starts from here. This tactic has become known as the "Dark Web".

The Dark Web-What Is It?

When we access online E-Commerce sites, we are accessing them through the primary interface of our Web Browser. Through this, we can type in the domain name of the online store, and within seconds it will take us there. But, believe it or not, this domain address is actually broken into a series of numbers, known specifically as an "Internet Protocol" ("IP") address.

So for example, if you were to type in the domain name of a popular online store, such as Overstock.com, it gets immediately transmitted to a series of specialized servers known as the "DNS System". From here, the domain then gets broken down into its IP address, in this case for overstock.com, it is 173.241.155.0.

Once this information is known, the DNS System then redirects you to the specific Web Server where this IP Address is hosted, thus enabling you to see the overstock.com online store.

But however, this is just one part of the vast expanse of the Internet that we are accessing. In other words, this is the portion of the World Wide Web which can be seen and accessed by all. It is very easy to determine the IP Address of a specific domain, and found which Web Server is actually hosting it. This part of the Internet is known as the "Surface Web".

Also, this is the one area of the Internet which is available to the major such engines (such as Google and Yahoo) so that the millions of websites which are available can indexed and ranked. But, there is another part of the Internet called the "Deep Web".

Although it is sinister sounding, in reality, it is not. This is that part of the Internet which cannot be recognized by the major search engines, and in fact many of the public websites can still be found in this area of the Internet, but the IP Addresses cannot be easily determined. Examples of this include using Google Docs for document collaboration and sharing.

But, drilling down further, there is a subcomponent of the Deep Web known as the "Dark Web", and yes, as evil as it sounds, it is literally that. This is that one realm of the Internet which is totally obscured and hidden from the realm of the public.

Also, this very murky part of the Internet can only be accessed by specialized software. For example, in order to gain access, you would have to download and use a package known specifically as "Tor". In order to keep all access points covert, rather than going to the DNS System to get to a requested website, you take a very random path to it which is full of encrypted connections which ultimately will mask your location and identity.

In other words, rather than taking a straight path, Tor uses what is known as "Onion Routing" to keep you bouncing through various and many covert network based nodes so that nobody can discover the path from where you have started or the destination you end up at in the Dark Web.

What the Dark Web Contains

To some degree or another, we have all heard of Phishing attacks. This is essentially when you get an E-Mail from an individual or an organization you probably never knew of before. The purpose of these messages is to lure you to clicking onto a link which will take you to a phony site.

But in these messages, there are usually telltale signs that it is a spoof, by the misspellings in the content, a subject line which does not make grammatical sense, a lack of contact information in the signature, etc.

But with the Dark Web, you can also be lured into going to fake a website which looks like the real thing. In these particular instances, if the Cyber hacker knows how to cover his or he tracks, the e-mail message will look just as authentic. The link provided will also, for example, take you to an online store which is completely phony, but looks like the real thing in every way.

But the difference here, is that since the IP Address is totally invisible to the outside world, there is absolutely no way track down on which Web Server the phony online store is being hosted on. As a result, once you submit your credit card information and other personal data, it is gone for good, and you could very well become a victim of Identity Theft.

The worst part of this is that you may know what happened to you until years later.

There are other equally worse aspects which the Dark Web contains as well, examples which include the following:

1) You can purchase large quantities of illicit drugs. A digital store, known as the "Silk Road", based in the Dark Web, just recently conducted $200 Million worth of illegal drug transactions over a two-year time span.
2) You can also purchase various types and kinds of counterfeit currency. In one particular instance, $600 can get you $2,500 in counterfeit U.S. notes, with the promise made by the seller that it will pass all of the counterfeit tests which are used today by law enforcement.
3) You can obtain firearms, ammunition, and other types of explosives. It is very easy to obtain them, and at a low cost. In particular, you can get easily C4 explosives. The vendors from the Dark Web ship these products in specially shielded containers (in order to avoid being picked up by X Rays), and the weapons components are often packaged in such items as toys, medical instruments, and electronic devices.
4) You can even hire a hitman. One such company that has these services in the Dark Web uses the advertising "Permanent solutions to common problems".
5) As bad as it sounds, one can even purchase live organs in the Dark Web. For instance, kidneys can go for $200,000, hearts at $120,000, livers at $150,000, and yes, a pair of eyeballs will cost $1,500 each.

But, in order to conduct any financial transactions in the Dark Web, the only accepted currency is that of the Bitcoin.

How to Protect Your Business from the Dark Web

It is imperative for businesses and corporations based in India to protect themselves from the adverse effects of the Dark Web. True, you can fortify your lines of defense with all of the security technology which is currently available on the marketplace, but it will all come down to the human equation-namely your employees.

There is that old adage that curiosity killed the cat, well the curiosity of your employees to surf the Dark Web using your IT infrastructure can bring your business down permanently in just a short period of time. Therefore, it is up to you, as the employer, to make your employees aware of the Dark Web, and the consequences of logging in to it from your resources.

You, the employer need to:

1) Inform:

   Educate your employees about the dangers of surfing and even using the Dark Web. Tell them that although they think their identities may be secure in the Dark Web, there is always an unmasked trail which is left behind which could further haunt them down the road.

2) Communicate:

   While you cannot control what your employee does outside of work hours, you need to keep reminding them that surfing the Dark Web using the IT infrastructure of the business or corporation will not be tolerated. Inform of the consequences, such as immediate termination and possible legal action.

3) Invest:

   Although it will not be cheap, it will be in your best interest to possibly hire an outside security consulting company to penetrate test your entire IT infrastructure to discover any vulnerabilities, and patch them up quickly. Also, they can assist with deploying covert countermeasures to keep tabs on your employees Web surfing habits while they are working.

4) Change:

   If possible, always try to use the latest security technologies to enhance the security of your perimeter. Using Two Factor Authentication (also known as "2FA"), keep having employees change their passwords at unannounced and random times. Also, consider using Biometric technology- This tool will positively confirm the true identity of your employees and any impostors which may be present, either in the Physical Accessor Logical Access aspects.

In the end, it is better probably not to surf the Dark Web. Even if you are doing it out of curiosity, after you log off, somebody will still be watching your footsteps, unbeknown to your knowledge. Leave this part of the world to the criminals and Cyber hackers. As an Indian company, it is best in your best and wisest interest to stay in the Surface Web part of the Internet.