Ultius, Inc.

Writing Samples

02 September, 2016

The Dark Web and Identity Theft

The Internet has a part called the Dark Web, and the Dark Web is a dangerous place with respect to identity theft. That statement may be a little confusing to most people, even as this is in fact a quite important personal security issue in these times. The purpose of the present sample essay provided by Ultius is to clarify and discuss the nature of the issue at hand here. Toward this end, the essay will begin by defining what the Dark Web itself is; and then it will proceed to a definition of identity theft. After this, the essay will delve into the nature of identity theft on the Dark Web. Finally, the essay will reflect on what people should do in order to protect themselves against this breach of their own personal information.

**Concept of the Dark Web**

To start with, Egan has indicated that "the Dark Web is a term that refers specifically to a collection of websites that are publicly visible, but hide the IP addresses of the servers that run them. Thus they can be visited by any web user, but it is very difficult to work out who is behind the sites. And you cannot find these sites using search engines" (paragraph 1). This is very different from the normal Internet (sometimes called the Clear Web), where websites are indexed by websites such as Google or Yahoo and it is usually a fairly simple process to figure out who is behind the websites, whether through IP addresses or other kinds of publicly available information. Relative to the normal Internet, then, the Dark Web is "shady," both in the sense that it is hidden from normal view and that the people who choose to hide themselves in such a way may tend to have motivations that are less than legal and/or moral in nature.

The nature of the Dark Web is such that websites there cannot be accessed in the same way that ordinary websites on the Clear Web are accessed. As Orborne has written: "You can't use standard access methods to gain entry into the Dark Web. The most common method is through the Tor network, an anonymous network created from nodes which disguise online activity. In order to use Tor, you need the Tor browser, and may also need to be issued an invitation to access certain domains" (2). In other words, there are levels of a kind of encryption in place that protect the Dark Web from the eyes of the general public. Indeed, most people (including the present writer) probably only have the vaguest idea of what Tor even is or how it works. And in addition to this prerequisite, some parts of the Dark Web are such that they can only be accessed upon being specifically invited to do so by persons who already have the access credentials for those sites.

For the sake of clarity, it is perhaps worth mentioning here that while the terms Dark Web and Deep Web are sometimes used interchangeably, they do not technically refer to the same thing. Essentially, the Dark Web could be understood as a subset of the Deep Web: if the Deep Web were a big circle, then the Dark Web would be a little circle within that big circle. As Egan has indicated: "The 'Deep Web refers to all the pages that search engines cannot find. Thus the 'Deep Web' includes the 'Dark Web', but also includes all user databases, webmail pages, registration-required web forums, and pages behind paywalls. There are huge numbers of such pages, and most exist for mundane reasons" (paragraph 5). The Dark Web, on the other hand, consists of that part of the Deep Web that has been intentionally and purposefully hidden by the people responsible for those pages, and not simply as a result of standard procedures on the normal Internet. Of course, this raises the question of what motivations people on the Dark Web could have for concealing themselves in this manner.

**Concept of Identity Theft**

According to Consumer.gov, "Identity theft is a serious crime. Identity theft happens when someone uses information about you without your permission. They could use your: name and address, credit card or bank account numbers, Social Security numbers, medical insurance account numbers" (paragraph 1). The Internet has proven to be fertile ground for the proliferation of identity theft. For example, criminals have used tactics such as pretending to be a respectable company (such as PayPal) and sending out e-mails requesting personal information from the Internet user. Or, the criminal could set up credible-looking websites accessing for personal information, and the Internet user may in good faith provide that information. This has become very problematic with the Internet in general, given that there are so many actual professional sites that require the user to provide this kind of information on website forms. Internet users may thus have by now gotten used to thinking of this as normal and thus fail to take the appropriate precautions regarding such sensitive information.

**Identity Theft on the Dark Web**

It may be worth beginning with a specific case in order to better illustrate how identity theft can operate on the Dark Web. Bailey has written the following: "In October 2013, Vietnamese national Hieu Minh Ngo was indicted on charges that he managed an international identity theft scheme. Ngo is the creator of a website called superget.info, which lets users search the Social Security numbers, birthdates, and other identity assets of millions of Americans" (paragraph 1). Ngo hosted a site where other criminals could literally buy all of this information for a price, and then use that information for various personal purposes—whether to steal money from the targets, file fraudulent documents with governments, or so on. There exists an actual underground virtual market for such personal information (see Heisler).

At this point, one may well wonder how such information finds its way onto the Dark Web in the first place. The simple answer to this question would be as more and more legitimate sites ask for personal information from Internet users, and as more and more data on Internet users is gathered as a matter of course, the risk of personal information ending up in the wrong hands tends to grows exponentially. As Manning (qtd. in Bailey) has suggested: "Facebook has started tracking a user's Internet activity no matter where they go on the Web. As all of that information is collected and collated, the profiles get more complete and the databases get more detailed—and the more information is bought and sold, the odds of it getting into the wrong hands grow" (paragraph 5). In short, it would seem that not only are people not taking adequate care of their personal information, we also now live in a society that makes it increasingly difficult to protect such information in the way that it should be protected.

Bleau has indicated that the cybercriminals who operate on the Dark Web are quite sophisticated, and that they often function in the same way that normal legal businesses function: for example, "cybercriminals selling stolen accounts and credit cards in the underground have their own blowout sales. Fresh off a data breach, stolen cards can go for upwards of $50 or $100, but once the supply floods the market or the data gets stale, a 'clearance' sale will ensue with prices going down to under $1 a card in some cases" (paragraph 2). In short, the black market for personal information on the Dark Web functions very much like an alternative economy, and the people in charge of it would seem to be quite competent at what they are doing, including evading the eyes of the general public and the relevant legal authorities. In short, this threat to personal information is no joke; and every Internet user (which is to say, pretty much everyone by now) should be aware of the risks that are involved when he gives personal information out to any party.

It would seem that one of the hottest personal information commodities on the Dark Web at the present time would be medical records. This is because "on the dark web, complete medical records typically contain an individual's name, birthdate, social security number, and medical information;" and this is far more valuable on the Dark Web than simple credit card numbers, due to the fact that whereas credit cards can be easily cancelled, "to change a social security number is no easy feat" (Farr, paragraph 5). Moreover, it is frightening to think about how easily one's own medical record could in fact get stolen. All it would take is someone with the adequate skills to hack a given hospital's database, or some unscrupulous insider who could literally just steal the hard drives containing the relevant information. For how valuable personal information is, the protections surrounding that information have clearly gotten quite weak within the context of contemporary society.

**Reflection on Protection**

This discussion leaves us with the question: what can people do, in order to protect their own personal information from getting into the hands of predators on the Dark Web? Unfortunately, the answer to this question is not an easy one; and in part, this is because of how little awareness people in general have about the functioning of the Dark Web. Indeed, most people do not even know it exists; and even those who do only know a little about how it functions. This is why Manning (qtd. in Bailey) has indicated that "little is known about Darknet and its potential uses, and the number of Darknet sites and the individuals using them is largely unknown. . . . Academicians and researchers can help us provide more information on Darknet activities" (paragraph 8). In other words, in order to protect themselves against identity theft on the Dark Web, people would first of all need to develop greater knowledge and awareness regarding the Dark Web itself.

It is seldom if ever the case, though, that people directly give personal information to agents on the Dark Web. Rather, what happens is either: one, people fall for scams on the Clear Web or the Deep Web (that is, they give personal information in response to fraudulent websites or e-mails); or, two, responsible parties who have requested personal information fail to protect that information in an adequate way, with the result that unscrupulous thieves are able to hack and/or otherwise obtain that information for their own Dark Web uses. In principle, there is really no way for people to protect themselves against this second issue except to take more care with respect to when and why they give out their personal information to anyone. The basic principle here is that the more people have even authorized access to that personal information, the greater the chances of something going wrong, somewhere, and that information being leaked to criminal parties. Clearly, though, this would be easier said than done, given the increasing prevalence of the Internet and the growing nature of universal surveillance within contemporary society.

**Conclusion**

In summary, the present essay has consisted of a discussion of identity theft on the Dark Web. After defining the relevant concepts, the essay delved into the nature of the problem itself. An important conclusion that has been reached here is that little is currently known about the Dark Web thus far, and moreover that even if more were known about it, the current nature of information sharing on even the normal Internet does not bode well for keeping criminals' hands off of personal information in the long run. That is, given how readily information is shared or gathered these days, it at some point becomes almost likely that some unauthorized party will find some way to obtain that information. This conclusion is not optimistic, and it potentially points toward the need for reforms in Internet culture in general.

Works Cited

Bailey, Tricia C. "Identity Theft and the Underground Economy." University of Texas at Austin. n.d. Web. 17 Jul. 2016. <https://identity.utexas.edu/id-perspectives/identity-theft-and-the- underground-economy>.

Bleau, Heidi. "The Economics of Identity Theft in the Dark Web." *RSA.* 18 Dec. 2015. Web. 17 Jul. 2016. <https://blogs.rsa.com/the-economics-of-identity-theft-in-the-dark-web/>.

Consumer.gov. "Avoiding Identity Theft." Author, n.d. Web. 17 Jul. 2016.

<https://www.consumer.gov/articles/1015-avoiding-identity-theft>.

Egan, Matt. "What Is the Dark Web?" *PC Advisor.* 28 Apr. 2016. Web. 17 Jul. 2016.

<http://www.pcadvisor.co.uk/how-to/internet/what-is-dark-web-how-access-dark-web- deep-joc-beautfiulpeople-3593569/>.

Farr, Christina. "On the Dark Web, Medical Records Are a Hot Commodity." 7 Jul. 2016. 17 Jul. 2016. <http://www.fastcompany.com/3061543/on-the-dark-web-medical-records-are-a- hot-commodity>.

Heisler, Yoni. "Here's How Much Your Stolen Data Is Worth on the Dark Web" *BGR.* 30 Nov. 2015. Web. 17 Jul. 2016. <http://bgr.com/2015/11/30/dark-web-stolen-data/>.

Osborne, Charlie. "10 Things You Didn't Know about the Dark Web." *ZDNet.* 12 Oct. 2015. Web. 17 Jul. 2016. <http://www.zdnet.com/pictures/10-things-you-didnt-know-about- the-dark-web/>.

Citation information

You are free to use this sample work for reference and research purposes. However, you **must cite it** and provide attribution to the author. The citation is provided below in MLA format.

Ultius, Inc. “The Dark Web and Identity Theft.” *Free Writing Samples | Ultius*. 02 Sep. 2016. [Web.](https://www.ultius.com/explore/writing-samples.html)

If you need help with MLA style, please visit the [Ultius citation style help section](https://www.ultius.com/help/citation-styles/mla-style.html). Thanks for playing fairly.