

Beware the Dark Side of the Web

Save to myBoK

Unless they know exactly what to look for, most Internet users wouldn't know that a "Dark Web" exists or what it is—let alone the potential for harm that can be done with it.

But the dark side of the web is out there, and its proprietors want your medical information.

In short, the Dark Web—or "deep web," as it is known to cyber security professionals—refers to a class of content that has been intentionally hidden and is not indexed by search engines like Google, according to a new report titled "The Impact of the Dark Web on Internet Governance and Cyber Security."¹

Websites on the Dark Web have addresses that end with .su and .so, rather than .com or .org. As one might suspect, these sites are hidden because would-be criminals use them to sell illegal products—including Social Security numbers, weapons, drugs, and pornography.

Even though the Dark Web hasn't become an epidemic problem yet, the healthcare industry does need to be on alert, according to security experts. The Dark Web has become a popular domain for sales of protected health information (PHI) and Medicare numbers. A recent National Public Radio (NPR) story about healthcare data on the Dark Web offered dire predictions about the security of that information.² The financial services sector has made strides in protecting financial data, but at least one expert says healthcare is nowhere near as prepared.

In the NPR piece, healthcare security expert Jeanie Larson warned that cyber security standards for hospitals and other healthcare providers are too low. "They don't have the internal cyber security operations," Larson says, noting that some providers interpret HIPAA too loosely and avoid encryption practices. "A lot of healthcare organizations that I've talked to do not encrypt data within their own networks, in their internal networks," she said.

If healthcare security professionals don't take the proper steps to protect their data, the industry can expect to see breaches as big as the recent Anthem breach—which exposed the health information of 80 million people—to become much more common, and possibly see that data float onto the Dark Web for sale.

Notes

1. Chertoff, Michael and Toby Simon. "The Impact of the Dark Web on Internet Governance and Cyber Security." Global Commission on Internet Governance. February 2015. https://ourinternet-files.s3.amazonaws.com/publications/GCIG_Paper_No6.pdf.
2. National Public Radio. "The Black Market For Stolen Health Care Data." February 13, 2015. www.npr.org/blogs/alltechconsidered/2015/02/13/385901377/the-black-market-for-stolen-health-care-data.

Article citation:

Journal of AHIMA Staff. "Beware the Dark Side of the Web" *Journal of AHIMA* 86, no.5 (May 2015): 80.

