@DeldigiKNOW

DigiKnow
CYBER SECURITY DEPENDS ON YOU

October 2018 Issue

Whooooooo's There?

October…. perhaps the spookiest month of them all. While hobgoblins, tricks and treats are child's play, this edition focuses on a real scary place, the Dark Web. Read on to find out why it's so frightening.

What Is The Dark Web?

CSO magazine explains: The dark web is a part of the internet that isn't indexed by search engines. You've no doubt heard talk of the "dark web" as a hotbed of criminal activity—and it is. Researchers Daniel Moore and Thomas Rid of King's College in London classified the contents of 2,723 live dark web sites over a five-week period a couple of years ago and found that 57 percent host illicit material.

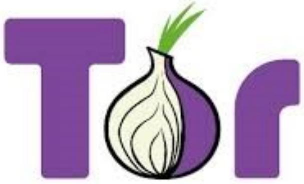
Accessing the dark web requires the use of anonymizing software. The Tor Browser (a modified Mozilla product) directs internet traffic through a free Tor volunteer overlay network, operated by thousands of volunteers around the globe, protecting user privacy by concealing your location and rendering your internet activities unidentifiable and untraceable.

Why is the Dark Web so attractive to cyber criminals? Take a look at what you can buy:

- Credit card numbers, drugs, guns, counterfeit money, stolen subscription credentials, hacked Netflix accounts and software that helps you break into other people's computers.
- Login credentials to a $50,000 Bank of America account for $500. Seven prepaid debit cards, each with a $2,500 balance, for $500 (express shipping included). A "lifetime" Netflix premium account goes for $6.

What Should I do?

The Tor Project Itself isn't Bad



The Onion Router (Tor) Project started as a core principle of anonymous communication developed by U.S. Naval Research Laboratory staff to protect U.S. intelligence communications online. DARPA developed onion routing further in the late 1990s. It was released to the public in 2004; the Electronic Frontier Foundation began funding its continued development. It remains particularly valuable in places hostile to free speech and has many legitimate users who simply wish to keep their internet activities private. There are full-text editions of rare books, whistleblower and political sites, and even a chess club.

The AARP Recommends Three Actions Assume all of your information is already on the internet in some form. We can worry about this, or we can take positive steps to make it harder for cyber scammers. To use stolen data to defraud you or someone else.

Cybersecurity experts and former hackers agree you should take these three steps to stay safe:

- **freeze your credit with all 3 major agencies,**
- **closely monitor all financial accounts, and**
- **use a password manager**.

Questions, comments or topic suggestions?
Email us at eSecurity@state.de.us

Visit the DTI Digiknow website for previous issues
eSecurity Newsletters

Department of Technology & Information
Delivering Technology that Innovates

Delaware Department of Technology and Information publishes and sends this newsletter to all network users because we need YOUR help to keep our network secure. If you are having problems viewing this message, accessing the links, or want to print a PDF copy, go to https://digiknow.dti.delaware.gov.