6 PLACES CROOKS STEAL (THEN RANSOM) YOUR DATA

Where there's an Internet connection, there's a datanapper. Here are six of their favorite hang outs.

THE DARK WEB

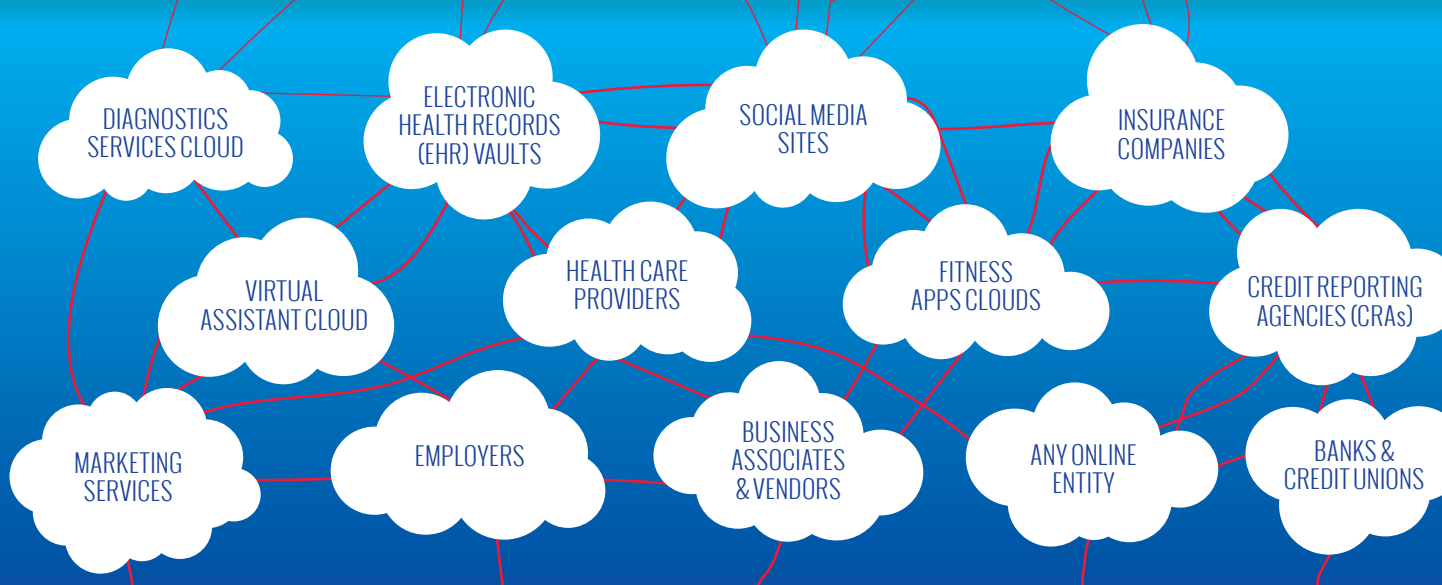
An aspiring thief's paradise, the Dark Web provides a wealth of valuable data and is a hotbed of training and tools.Because many victims lack file backups or workable data recovery plans, they desperately pay the ransom demanded for their data. It's why ransomware has become so popular... and so lucrative.

Ransomware sellers are making annual salaries over $100K.

THE INTERNET OF THINGS (IOT)

Tech giants like Microsoft employ engineers to patch vulnerabilities. It's what they do all day, every day. Smaller organizations and startups, though, often don't have those teams. Much of the IoT is being built by app designers and smart gadget innovators that create really cool stuff, but often without security or privacy controls, or even the ability to be patched.

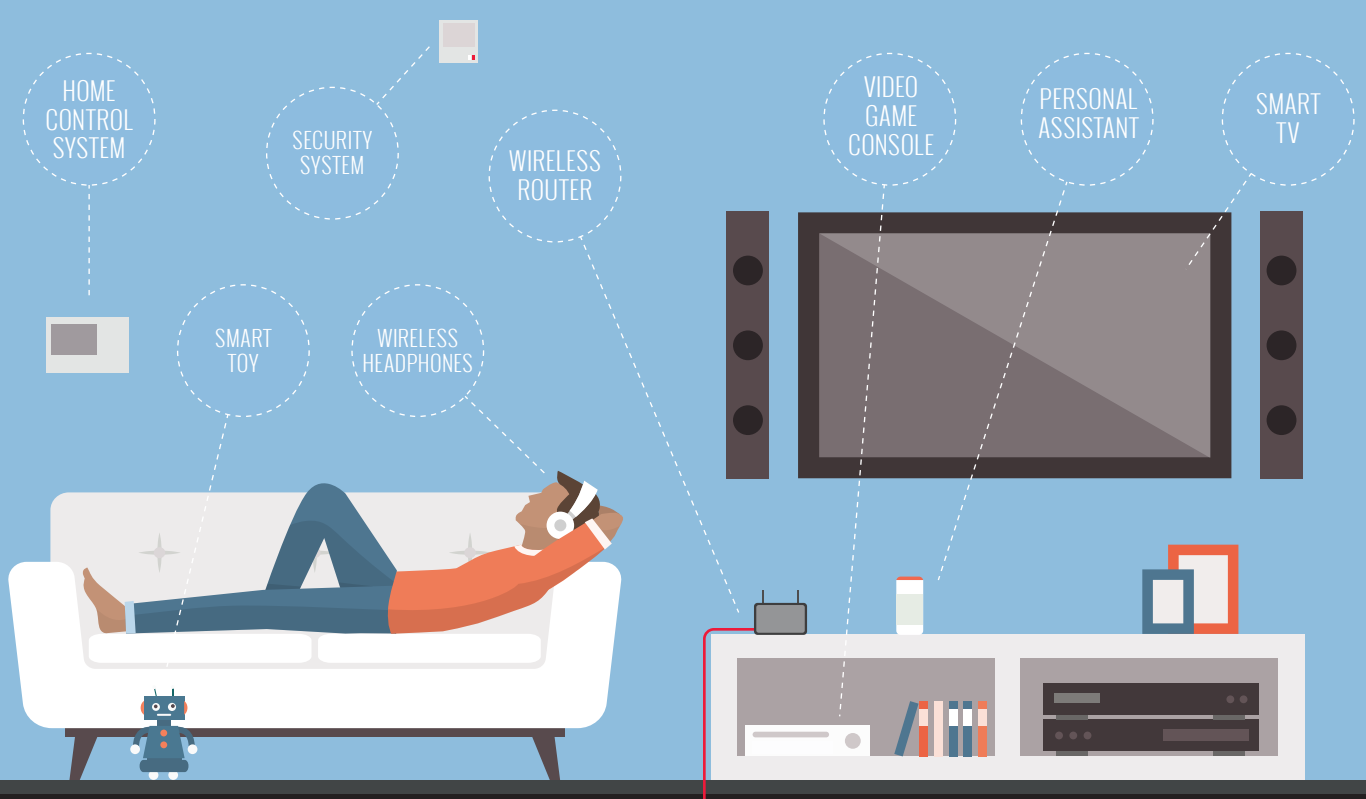
32% of IoT solution builders admit keeping the IoT secure is their greatest challenge.



HOME

Many of the smart gadgets in our homes offer zero security. A connected teddy bear exposed the emails and passwords over 820,000 users. A dog-walking app published addresses and lockbox codes on the Internet. Stolen data like this could turn crime from digital to physical in a hurry.

Ransomware can commandeer and steal data from baby monitors, thermostats, even home-security systems.



WORK

Workplace data thieves have honed their craft. They are deploying laser-targeted and artfully disguised phishing attacks that appear to come right from the C-suite. It's hard enough to secure the devices owned by a company, let alone those owned by employees.

67% of workers use their personal devices at work. Who else is seeing, or getting copies of, work data through those devices?

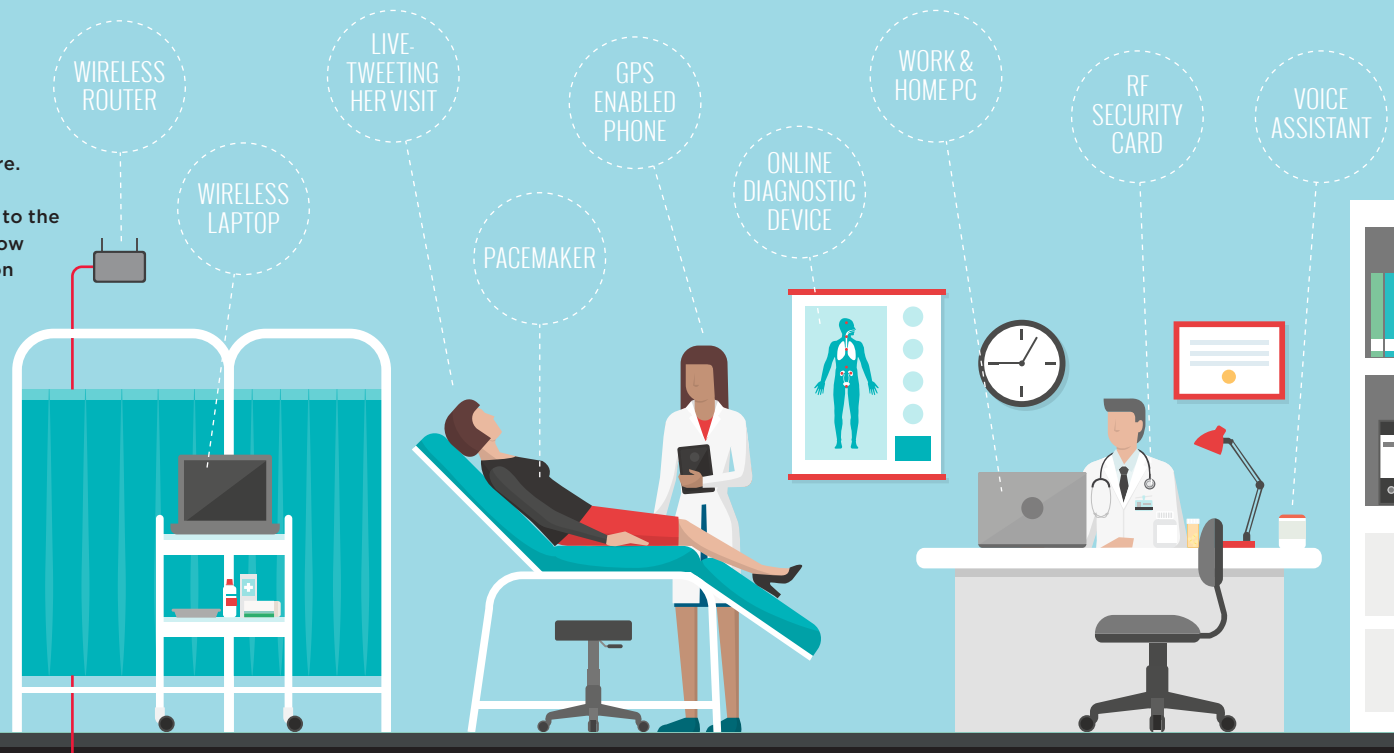
DOCTOR

72% of all health care malware attacks in 2016 were ransomware. The increased use of unsecured smart devices in practices adds to the threat. 23% of U.S. physicians now use voice assistants, like Amazon Echo, in their clinics. As they dictate your diagnosis, who else is listening?

A SSN sells for $1 on the Dark Web; a medical record sells for $1,000.

Only 17% of medical device makers take meaningful steps to build in strong security.

Only 5% of hospitals annually test medical device security.



STORE

15% of all ransomware attacks are on retail. Crooks love big-box merchants for two reasons: 1) Retailers house massive amounts of consumer data; 2) Retailers, especially online, operate 24x7. Even 30 seconds of downtime threatens profits, so many retailers are apt to pay ransom.

62% of retailers report a competitive advantage from using data and analytics.

HOW TO STAY SAFE

Datanappers love the way we live, always connected and happily over-sharing. While you shop, get a check-up, work or just watch streaming movies and chill, the bad guys are right there watching, waiting for you to drop your data. Your best defense against ransomware is three-fold:

1. **Know.** Be aware of who has your data and how they protect it, and know that unlimited others want the data on your smart devices.
2. **Patch.** Configure automatic updates.
3. **Back Up.** Get and stay on a consistent schedule, and make sure you can restore the data quickly.

PRIVACY PROFESSOR™
www.privacyprofessor.org

SIMBUS 360
INFORMATION SECURITY - PRIVACY - COMPLIANCE
www.SIMBUS360.com

SOURCES

The following are in the order for which they were listed above:

Here's How Much Your Personal Information Is Selling for on the Dark Web: https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/

The dark web: What your business needs to know: https://www.ftc.gov/news-events/blogs/business-blog/2017/10/dark-web-what-your-business-needs-know

Ransomware is now big business on the dark web and malware developers are cashing in: http://www.zdnet.com/article/ransomware-is-now-big-business-on-the-dark-web-and-malware-developers-are-cashing-in/

The Seven Habits of Highly Effective Ransomware Attacks: https://blog.sonicwall.com/2017/04/the-seven-habits-of-highly-effective-ransomware-attacks/

Dog-Walking App Exposed Home Addresses and Lockbox Codes: https://www.wsj.com/articles/dog-walking-app-exposed-home-addresses-and-lockbox-codes-1515524881

23 BYOD Statistics You Should Be Familiar With: http://www.ingrammicroadvisor.com/data-center/23-byod-statistics-you-should-be-familiar-with

Synopsys and Ponemon Study Highlights Critical Security Deficiencies in Medical Devices: https://www.prnewswire.com/news-releases/synopsys-and-ponemon-study-highlights-critical-security-deficiencies-in-medical-devices-300463669.html

Nightmare scenario: Only 5% of hospitals annually test medical device security: http://www.healthcareitnews.com/news/nightmare-scenario-only-5-hospitals-annually-test-medical-device-security