your energy partner®
OPPD
Omaha Public Power District

SHIELD
SECURE
HANDLE
INVOLVE
ELIMINATE
LEARN
DEFEND
Information Protection Newsletter

The Biggest Cyber Threats to Watch Out for in 2019

By Security Magazine: Solutions for Enabling and Assuring Business

Experts from The Chertoff Group, a global security advisory firm that enables clients to navigate changes in security risk, technology and policy, developed a list of the biggest cyber threats to watch out for in 2019.

Cryptojacking

If the recent and explosive growth of ransomware is an indication of anything, it is that criminal organizations will continue to employ malware for profit. Cryptojacking, otherwise known as "Cryptomining malware", uses both invasive methods of initial access, and drive-by scripts on websites, to steal resources from unsuspecting victims. Cryptojacking is a quieter, more insidious means of profit affecting endpoints, mobile devices, and servers: it runs in the background, quietly stealing spare machine resources to make greater profits for less risk. Due to its ease of deployment, low-risk profile, and profitability TCG posits that this trend will continue to increase in 2019.

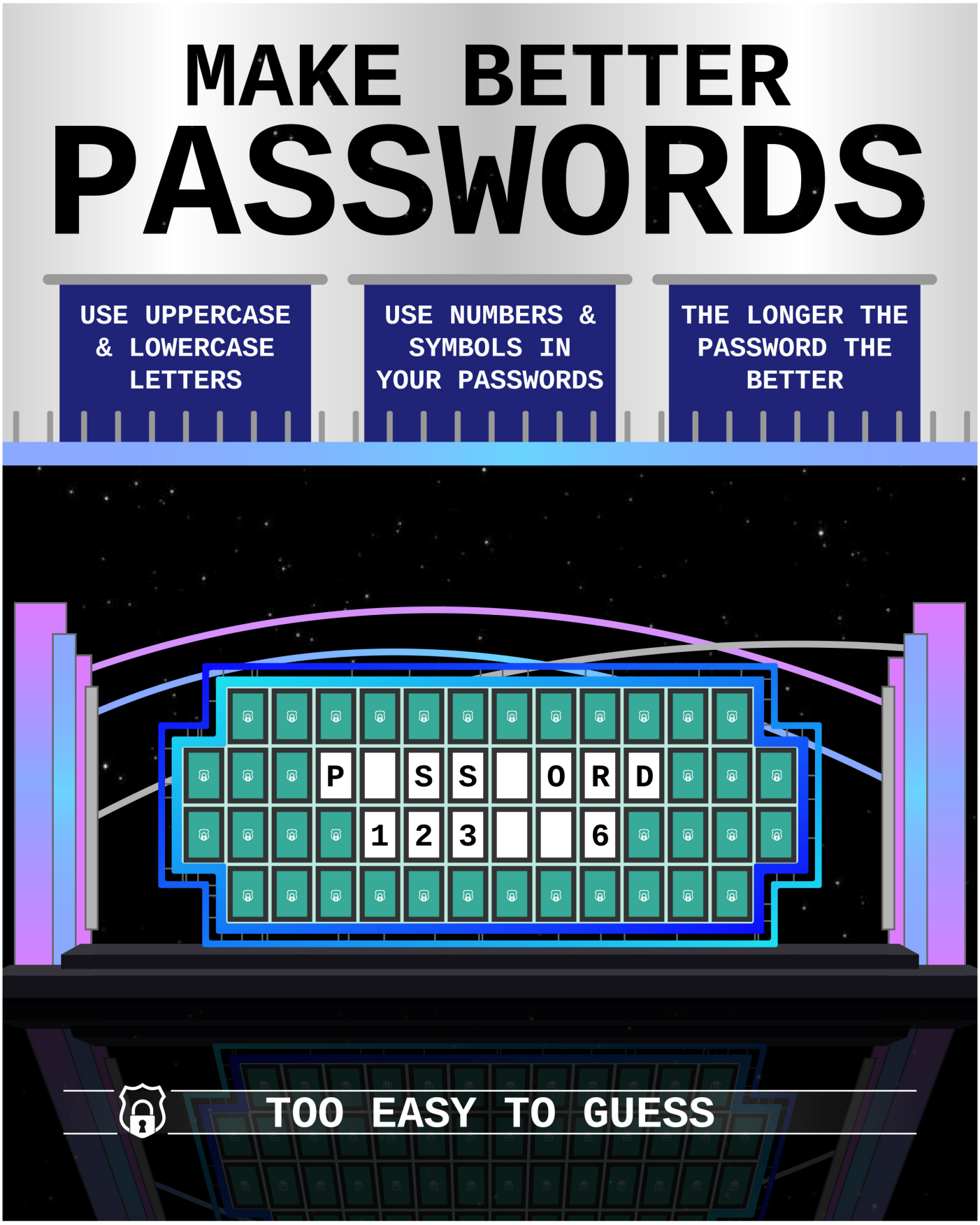
Software subversion

While exploitation of software flaws is a longstanding tactic used in cyber attacks, efforts to actively subvert software development processes are also increasing. For example, developers are in some cases specifically targeted for attack. Malware has also been detected in certain open source software libraries. As software code becomes more complex and dynamic, the opportunities for corruption increase as well. In 2019, we will see a continued increase in the use of third-party applications or services as the "back channel" into networks through the corruption of third-party firmware/software (and updates thereof); such back channels can bypass traditional protective and detection capabilities in place to prevent externally-based incidents and infecting the corporate network.

Rise in attacks to the cryptocurrency ecosystem

"Why do people rob banks? That's where the money is." Use of cryptocurrencies for everyday transactions is becoming commonplace, and we will continue to see a related rise in attacks against individuals and organizations who use cryptocurrency as an increasingly standard element of their business operations and transaction options.

Read more at https://www.securitymagazine.com/articles/89581-the-biggest-cyber-threats-to-watch-out-for-in-2019



http://cybersafework.com/

CYBER SAFE WORK

Creating A Culture Of Security

Scam of the Week: Black Friday & Cyber Monday Alert

We have been warning against these types of scams for years and the bad guys are at it again. The team at RiskIQ summarized it pretty well this time:

"Ever the opportunists, threat actors set up their operations where the money is; and in the case of the Black Friday and Cyber Monday phenomena, it's e-commerce. According to Adobe Digital Index, in 2017, online shoppers stuffed e-commerce cash registers with more than $19.6 billion in sales through the Black Friday weekend—a more than 15 percent increase over 2016.

"With more people than ever poised to partake in this year's November shopping frenzy, attackers will capitalize by using
the brand names of leading e-tailers to exploit users looking for Black Friday deals and coupons by creating fake mobile apps and landing pages to fool consumers into downloading malware, using compromised sites, or giving up their login credentials and credit card information."

The folks at RiskIQ have a great overview that shows all the holiday shopping risks this year. They specifically warn against domain infringement:

"Domain infringement targeting brands, employees, and customers is a prolific, effective tool in the hands of attackers and has only grown worse in recent years due to the opening of thousands of new gTLDs, the growth of free and cheap domain registration services, and attack techniques like domain shadowing.

Because corporate attack surfaces are changing, threat actors are also changing their methods. Since business has moved many critical financial and data transactions beyond the firewall to the open internet, attackers are following suit, directly scamming end-users with high-volume phishing campaigns against consumers or targeted spear-phishing campaigns attempting to fool corporate employees.

These attacks are cheap to execute, and they are proving to be incredibly efficient in breaching sensitive data—a recent query of the branded terms of 20 Fortune 100 companies in RiskIQ's domain infringement detection revealed 37,000 probable instances of domain infringement over a two-week period or 1,850 incidents per brand."

Read more at https://blog.knowbe4.com/scam-of-the-week-black-friday-cyber-monday-alert