@DeldigiKNOW

DigiKnow
CYBER SECURITY DEPENDS ON YOU

January 2019

Cyber Challenges In 2019

The new year brings opportunities and challenges in cyber security. Read predictions from CSO Magazine and other cyber security experts about trends and threats in 2019.

Cyber trends from CSO Magazine

Ransomware **-** will taper off as criminals shift to other ways to generate revenue. "While ransomware will still be a problem, it will be more of a focused, targeted attack," says Steve Ragan, CSO's senior staff writer. He cites the declining number of ransomware attacks. According to Kaspersky, the number of users who encountered ransomware in 2017 and 2018 fell by nearly 30 percent over the 2016 to 2017 time period.

Data Protection - Last year, CSO predicted that the European Union (EU) would quickly punish a few companies in violation of its General Data Protection Regulation (GDPR) to make an example of them. That didn't happen. The threat of penalties over compromised personal information will still have a huge effect in 2019.

Privacy - Rising concern over how companies use and protect personal information will encourage many Americans to hold those companies more accountable. "The reaction by consumers to constant security breaches and other unethical information disclosures (e.g., Facebook) leads U.S. consumers to demand more default privacy and control over their own information," says CSO contributor Roger Grimes.

Privacy Laws - Expect to see an effort to enact privacy laws similar to GDPR nationally in 2019. The California Consumer Privacy Act has already passed into law and goes into effect in 2020. On November 1, Sen. Ron Wyden introduced a bill titled the Consumer Data Protection Act (CDPA), which has stiff penalties, including jail time, for privacy violations. The California Consumer Privacy Act has already passed into law and goes into effect in 2020.

Visit the DTI Digiknow website for previous issues

eSecurity Newsletters

Voice Phishing Scams

Voice Phishing Scams (vhishing) are becoming more sophisticated, according to Brian Krebs, a respected author and lecturer in the cyber arena. In KrebsOnSecurity he writes:

Most of us have been trained to be wary of clicking on links and attachments that arrive in emails unexpected, but it's easy to forget scam artists are constantly dreaming up innovations that put a new shine on old-fashioned telephone-based phishing scams. Think you're too smart to fall for one? Think again.

It's not just banks and phone companies that are being impersonated by fraudsters. Reports on social media suggest many consumers also are receiving voice phishing scams that spoof customer support numbers at Apple, Amazon and other big-name tech companies. In many cases, the scammers are polluting top search engine results with phony 800-numbers for customer support lines that lead directly to fraudsters.

Just as you would never give out personal information if asked to do so via email, *never give out any information about yourself in response to an unsolicited phone call*. Likewise, if contacted by a bank or credit card company regarding "fraud on your account" or other urgent issue, be cautious. If a call has you worried that there might be something wrong and you wish to call them back, don't call the number offered to you by the caller. If you want to reach your bank, call the number on the back of your card. If it's another company go to the company's site and look up their main customer support number.

Read more here: https://krebsonsecurity.com/2018/10/voice-phishing-scams-are-getting-more-clever/

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

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.