Case Studies

Easily Cracked Passwords Put Systems at Risk

Following the Colonial Pipeline attack that exploited a weak password to cause gas shortages along the East Coast, the U.S. Department of the Interior conducted an internal test of the passwords throughout the Department. They were able to crack 21 percent of active user passwords, including accounts with elevated privileges. The most commonly re-used password was Password-1234, and five of the ten most re-used passwords included a variation of "password" combined with "1234".

Ransomware Attack Closes School

A ransomware attack shut down a school district's network, causing the district to cancel classes for a day. The school's cybersecurity team isolated the attack and shut down the network before information could be affected or compromised, but the shutdown affected basic functions necessary to run the school. The cause was identified as an encrypted download.

Callback Phishing Attempts Increase by 625%

Think that phishing e-mails only want you to open a link? A tactic on the rise is to e-mail a phony invoice, often for a pricey monthly subscription, along with a phone number to call if you have questions. Once called, the attacker guides you to install a tool on your computer that gives them remote access to do as they like with your data. Your e-mail filters are less likely to block the e-mail since it does not contain links or malicious code, and the use of legitimate tools makes the intrusion more difficult to detect.

Navy Spy Sentenced to 232 Months in Prison

As a nuclear engineer with the Department of the Navy, Jonathan Toebbe worked with and had legitimate access to Restricted Data. Toebbe attempted to establish a covert relationship with a foreign government to sell Restricted Data and began corresponding via encrypted e-mail with an undercover FBI agent. Toebbe made dead drops of data cards containing Restricted Data, providing the decryption key to the undercover agent upon payment.