your energy partner®
OPPD
Omaha Public Power District

SHIELD
SECURE
HANDLE
INVOLVE
ELIMINATE
LEARN
DEFEND
Information Protection Newsletter

BEWARE - Ransomware Impacts are Real

By CNN: Florida city to pay $600,000 ransom to hacker who infected government computer systems with ransomware

A Florida city is paying $600,000 in Bitcoins to a hacker who took over local government computers after an employee clicked on a malicious email link.

Riviera Beach Florida government officials voted this week to pay the ransomware fee of 65 Bitcoins to the hacker who seized the city's computer systems, forcing the local police and fire departments to re-vert back to writing down the hundreds of daily 911 calls on paper due to their network being down.

The 65 Bitcoins, which equals $600,000, will come from the city's insurance, officials said. Once the ransom payment is made, they hope to get access back to the data encrypted by the hacker.

Targeted ransomware attacks on local US government entities -- cities, police stations and schools -- are on the rise, costing millions as some pay off the perpetrators in an effort to untangle themselves and restore vital systems. The most popular and easiest way to take control over networked computers in the modern world is by phishing attacks. When a user is phished, a fraudulent email is delivered to them, and if a link is clicked it can give an attacker an entry point into your system and your company's network. Most phishing attempts come

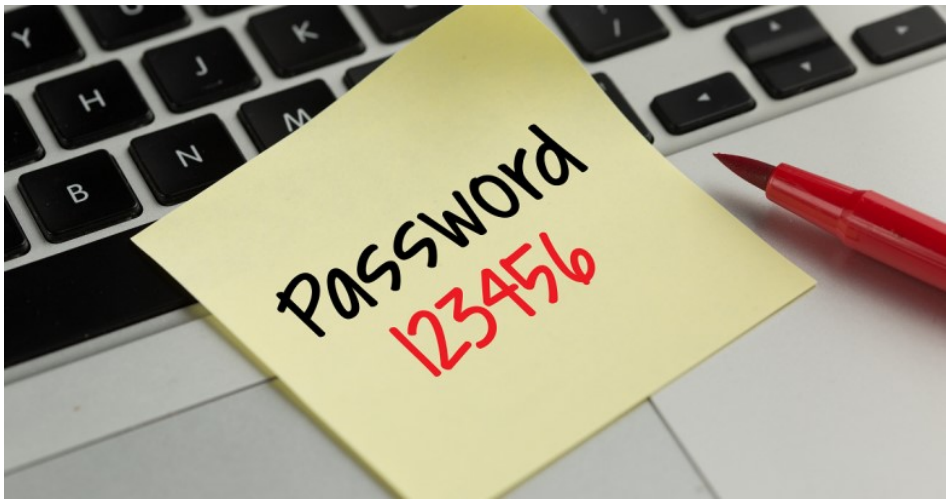
from 3rd party vendors that already have established trust built up with the larger company. Once the 3rd party vendor is hacked, it's an avenue into the larger companies front door. People with unsafe passwords are more unsecure, and more likely to be hacked by people with malicious intent. Remember to keep your passwords complex, safe, never reuse them, and don't reuse the same password across multiple web-sites or other user accounts.

The FBI stated that 1,493 ransomware attacks were reported in 2018. Victims, including individuals, paid $3.6 million to hackers. That figure doesn't include estimates for lost business, time, wages, equipment or services from a third party. Do your part to keep the network secure and remain skeptical while check-ing email and surfing the internet.

For more information: https://www.cnn.com/2019/06/20/us/riviera-beach-to-pay-hacker/index.html

Scam of the Week: "Most Hacked Passwords" List is Growing

Names, soccer players, musicians and fictional characters make up some of the worst passwords of the year, according to the U.K. government's National Cyber Security Center (NCSC).



But nothing beats "123456" as the worst password of all.

It's no shock to any seasoned security pro. **For years, the six-digit password has been donned the worst password of all, given its wide usage. Trailing behind the worst password is surprise, surprise — "123456789".**

The NCSC said **more than 30 million victims use those two passwords alone**.

"**We understand that cyber security can feel daunting to a lot of people**, **but the NCSC has published lots of easily applicable advice to make you much less vulnerable**," said Dr. Ian Levy, NCSC's technical director. "**Password re-use is a major risk that can be avoided — nobody should protect sensitive data with something that can be guessed, like their first name, local football team or favorite band**."

Weak passwords are a problem. Not only can they be easily guessed by bots trying to break into your account, they can be easily cracked if they're ever stolen from the company in a data breach. Weak passwords are often defaults in the internet of things, making it easy for botnets to quietly break into your smart devices and hijack them for nefarious purposes. Help raise the defenses of your organization by making your password unique, and include numbers and symbols, and use a phrase that will be difficult to guess by others.

Weak Passwords = Weak Security

https://techcrunch.com/2019/04/21/hacked-passwords/

KEEP YOUR PASSWORDS

- CØMPLEX -

AND CHANGE THEM OFTEN

PASSWORD

SuGG3s+!ØnS

- ✓ UPPERCASE LETTERS
- ✓ LOWERCASE LETTERS
- ✓ NUMBERS
- ✓ KEYBOARD SYMBOLS
  SUCH AS ! * - () : | / ?

- ✗ YOUR FIRST OR LAST NAME
- ✗ REPEATED CHARACTERS
  AAA OR 555
- ✗ COMMON SEQUENCES
  ABC, CBA, 123, 321, QWERTY
- ✗ EASY TO GUESS PHRASE
  USA, NAVY, SAILOR

DO NOT LET ANY TWO ACCOUNTS HAVE THE SAME PASSWORD

- NEVER SHARE YOUR PASSWORDS WITH ANYONE! -

LOVED ONES

CO-WORKERS

PETS

DON'T MAKE YOURSELF AN EASY TARGET

Always remember to use complex passphrases, avoid reusing passwords on multiple accounts, and NEVER share your passwords so your accounts harder to breach by malicious attackers.

For more security tips see: http://insideoppd/Divisions/InformationTechnology/EnterpriseOperations/CS/Pages/SecurityAwareness.aspx