your energy partner®
OPPD
Omaha Public Power District

SHIELD
SECURE
HANDLE
INVOLVE
ELIMINATE
LEARN
DEFEND
Information Protection Newsletter

Poor Information Security Practices Expose 161 Million User Records

By SC Magazine

An exposed database on a MoviePass subdomain housing 161 million records was left unsecured and exposed credit card and customer card information on at least 60,000 of the ticket service's customers.

The database, which included expiration dates, names and addresses on some users as well as email and passwords, was discovered by SpiderSilk security researcher Mossab Hussein, according to a report from TechCrunch, which said the information may have been exposed for several months.

"Because a database was left publicly accessible, reportedly for months, at least 58,000 records related to MoviePass customers are vulnerable to misuse and abuse at the hands of cybercriminals," said Stephan Chenette, Co-Founder and CTO at AttackIQ. "At its peak, MoviePass boasted more than 3 million customers in June 2018, so it's entirely possible we'll see the number of impacted individuals grow exponentially."

And while it's a "bit unclear how many of these records included sensitive consumer data," said Jumio President Robert Prigge, "what we should all expect is that a healthy chunk of this data will ultimately find a happy home on the dark web."

Because "technically, this breach can be interpreted as the company giving away customer data for free" and because the exposed data included personally identifiable information and payment card details, it leaves "impacted customers vulnerable to future fraud or phishing attacks," said Arkose Labs CEO Kevin Gosschalk.

```
sed Users only!
rs MUST notify Sys/Ops.
                                         rcr ebx, 1
                                         bsr ecx, ecx
                                         shrd ebx, edi, CL
--- 10.2.0.0 ping statistics ---
1 packets transmitted, 1 packets received, +44 duplicates, [illegible] packet loss
round-trip min/avg/max/stddev   0.252/2.455/17.0/0/3.[illegible]
# ping -c 2 10.2.0.0 | grep "^64" | awk '{print [illegible] | sed
  's.:..g' | csh |& grep Address
Address:  10.2.1.3

# nmap -v -sS -O 10.2.1.3

Starting nmap V. 2.SNBETA25
Host 10.2.1.3 appears to be up [illegible]
Initiating SYN Stealth Scan against [illegible]
For OSScan assuming that port [illegible] is open [illegible] port 1 is closed and neither are
firewalled
Insufficient responses [illegible] sequencing (3), OS detection may be less
accurate
Interesting ports [illegible]
(The 1521 ports [illegible] shown below are in state: closed)
Port       [illegible]    Service
21/tcp     open          ftp
22/tcp     open          [illegible]
23/tcp     open          telnet
25/tcp     open          smtp
```

"Unlike credit cards, debit cards don't offer the same protection to customers. When a fraudulent transaction occurs on your credit card, you have lost no money and the issue will never impact your bank account. With a debit card, your bank account balance is directly affected from the moment the fraudulent transaction takes place. While the customers can put a hold on their cards, timing is the key in these types of situations. As this database was left publicly accessible, reportedly for months, companies must learn from MoviePass's mistake and implement a proactive approach to fraud prevention that safeguards their customers' data."

If the data had been masked, the information would still be accessible, but perhaps not so immediately valuable but if access rights were configured properly and appropriately, this discovery might never have been made and there would be no story in the first place. Always take an active role by asking how your vendors store and process your company's information. Read More: https://www.scmagazine.com/home/security-news/moviepass-database-exposes-161-million-records/

A potentially state-sponsored hacking campaign tried to phish U.S. utilities in July, researchers say—Cyber Scoop Reports

Hackers that may be state-sponsored tried to spearphish three companies in the U.S. utility sector last month, cybersecurity company Proofpoint said Thursday.

The malware-laced emails were sent from July 19 to July 25 and appeared to impersonate a national association that facilitates engineering exams, Proofpoint researchers said. A Microsoft Word document attached to the emails contained a remote access trojan capable of deleting files, taking screenshots, rebooting a machine, and deleting itself from an infected network, among other attributes.

Sherrod DeGrippo, Proofpoint's senior director of threat research and detection, told CyberScoop that her company blocked the spearphishing attempts on the three companies, which are Proofpoint customers. However, she said, "it is likely that this campaign extended to multiple utilities outside of our purview."

It is unclear who is behind the phishing operation. There are similarities between the macros used in this campaign and targeting carried out last year by a Chinese government-linked group against Japanese companies, Proofpoint said. Researchers and U.S. officials have tied the group, known as APT10 (advanced persistent threat), to China's civilian intelligence agency, and have blamed it for a series of data-stealing attacks on Western companies.

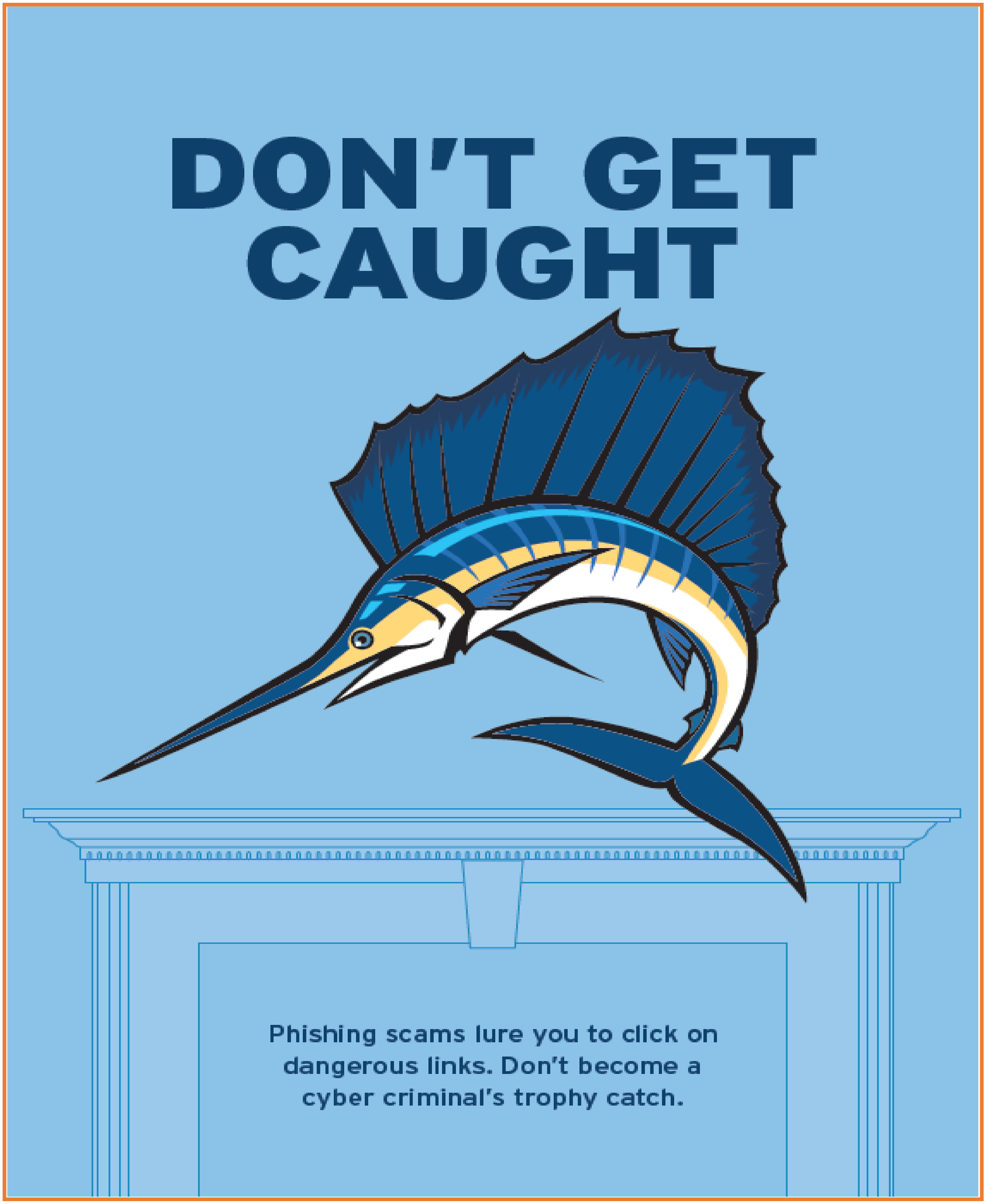
Proofpoint researchers Michael Raggi and Dennis Schwarz said the profile of the phishing campaign "is indicative of a specific risk to U.S.-based entities in the utilities sector. Phishing emails leveraged knowledge of the licensing bodies utilized within the utilities sector for social engineering purposes that communicated urgency and relevance to their targets."

The phishing emails flagged by Proofpoint purported to be from the National Council of Examiners for Engineering and Surveying, a South Carolina-based nonprofit.

"We are posting a notice on our website in case anyone else is affected by this issue, and we are sending email notifications to recent examinees to alert them to the issue and remind them that NCEES does not send exam results via email," Cox added.

The discovery comes as multiple government-affiliated hacking groups continue to take an interest in electric utilities and the oil and gas sector. In June, cybersecurity company Dragos warned that the notorious group behind the Trisis malware, which is designed to disrupt industrial safety systems, had expanded its targeting to include U.S. electric utilities. This is one more example of why employees and subcontractors must remain engaged while working online to help protect their employer's digital assets.—

Read More: https://www.cyberscoop.com/apt-10-utilities-phishing-proofpoint/


DON'T GET CAUGHT
Phishing scams lure you to click on dangerous links. Don't become a cyber criminal's trophy catch.

Phishing Scams are the most common ways that companies, people, and organizations are hacked. Keep a watchful eye, you could be the person to thwart a cyber attack.

https://www.consumer.ftc.gov/articles/how-recognize-and-avoid-phishing-scams