The Star (3/1/2022) Page 6

Ongoing cyber threats

Cybercriminals likely to hit more businesses, exploit digital payments in 2022.

AFTER years of data breaches exposing individuals' personal information, cyberthieves will increasingly use that information to attack businesses in 2022, according to the Identity Theft Resource Centre's predictions for the coming year.

"We also tracked a record number of data breaches and a steady flow of new victims of unemployment benefits identity fraud long after the enhanced benefits ended," said Eva Velasquez, president and CEO of Identity Theft Resource Centre.

Velasquez anticipates an increase this year in the number of people who have been victims of identity theft multiple times. And she warned of particular risk ahead as people change how they pay for things.

"Look for cybercriminals to take advantage of the shift to alternative digital payment methods, such as payment apps, digital wallets and peer-to-peer services," Velasquez said.

With cryptocurrency becoming increasingly popular, scammers will find new ways to steal from consumers, according to the resource centre, which is a US non-profit that tracks data compromises and provides free assistance to victims.

The centre's predictions for 2022 include:

- An accelerated shift from identity theft to use of already stolen personal information and credentials to commit identity fraud and attack businesses.
- Consumers may shift away from some online transactions and email communications due to the increasing problem of phishing, which is when cybercriminals use a fraudulent email or website to masquerade as a legitimate business or person.
- The effects of pandemic-related fraud will continue into 2024, with some fraud cases taking years to resolve and unemployment compensation fraud efforts likely becoming permanent.
- Ransomware, when hackers use malicious software to infect and lock a computer network and demand demand money to restore access, may surpass phishing as the top cause of data breaches.
- Supply chain attacks, which is when malware infects a single organisation that is linked to multiple others, will become more common.
- Single incident attacks will impact greater numbers of individuals, including social media account takeovers that victimise followers and networks.

"All of these trends point toward increases in identity fraud that will change consumer behaviours, revictimisation rates and pandemic-related identity crimes for years to come," Velazquez said.

"We expect to see these types of cyberattacks and who they target continue to evolve as they did in 2021."

The resource centre called for wider consumer education efforts and improved data protection.

Publicly reported data compromises in the US

Year	Events	Victims
2021	1,291	281.5 million
2020	1,108	310.1 million
2019	1,279	883.6 million
2018	1,175	2.2 billion
2017	1,529	1.8 billion
2016	1,105	2.5 billion
2015	785	318.3 million

– 2021 is of 30/9/21

Source: Identity Theft Resource Centre.

The number of publicly reported data compromises was already higher last year than in all of 2020. The centre's third quarter report shows that as of Sept 30, 2021, data compromises rose by nearly 17% over all of 2020. The report found that nearly 281.5 million people were victims last year.

There were 1,291 data compromise events in 2021, compared to 1,108 in all of 2020. The record is 1,529 in 2017.

In November, the resource centre released data showing that 16% of 1,050 US adult consumers surveyed took no action after receiving a data breach notice, according to the survey by the resource centre and DIG.Works, a consumer research company.

Fewer than one-third of survey respondents had frozen their credit at one time for any reason and only 3% did so after receiving a data breach notice, the survey found. – Journal-News, Hamilton, Ohio/Tribune News Service