

A SCAMMER'S CAROL

A review of scams past, present, and future



THIS MONTH'S TOPICS:

Scammings Past:

The Scam-World of the past

Scammings Present:

No gift like the present

Scammings Future:

Scam of the future (month)

Cyber Zen:

Reflection Section

December is more than just another month. It is a marking of the end of an era. A 31-day reminder to reflect on the old, and prepare for the new.

The cybersecurity world is no stranger to December. It is a time when many fraudulent cyber activities reach their peak, and new tricks get formulated.

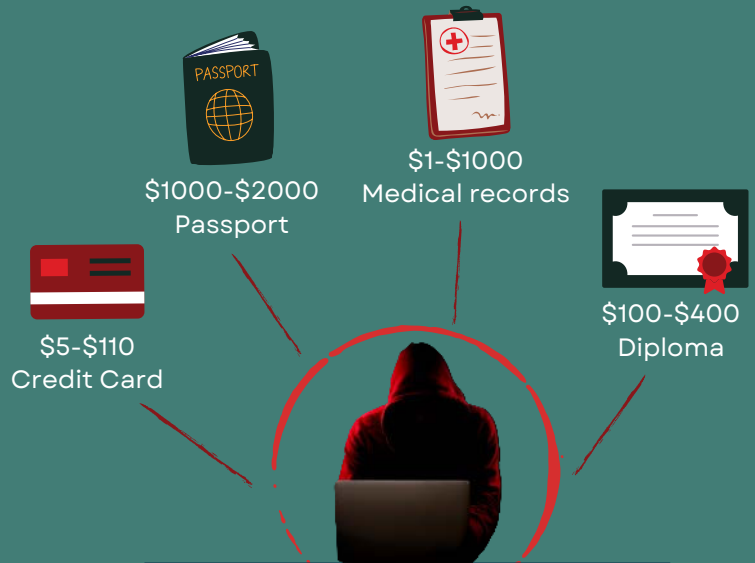
In this month's issue, we're going to review the past, present, and future of scamming. Helping you take the time this December to reflect, re-learn, and grow into the New Year as the vigilant, cyber-aware, non-link-clickers that we all aspire to be.



SCAMMINGS PAST

REFLECT

Cybercriminals grow more sophisticated with each year. By reflecting on the Scam-World of the past, you can better prepare yourself for the future.



CYBERCRIME - A TIMELINE



WHAT PII HAS BEEN WORTH ON THE DARK WEB



2017

2018

2019

2020

\$328 MILLION LOST TO IMPOSTER SCAMS

Of the reported imposter scams this year, 1 in 5 people lost a median range of \$500

ACCOUNT TAKEOVER GROWS

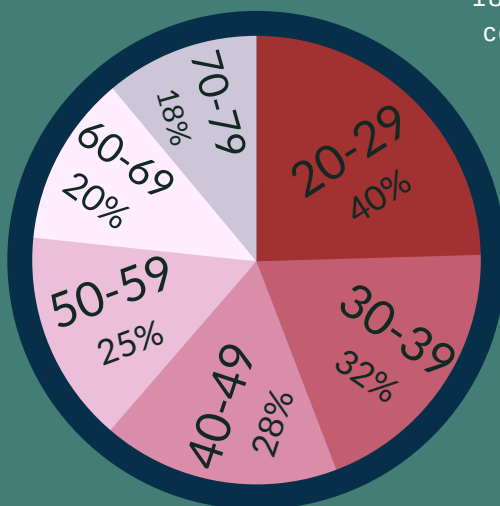
Reaching a four-year high, ATO tripled in 2018, resulting in over 5.1 billion in losses

RELATIVES COMMIT FRAUD AGAINST MINORS

A 2019 identity fraud report analyzing 1 million cases against minors, found that 18% of those crimes were committed by the child's relative

CYBERCRIMINALS TAKE ADVANTAGE OF PANDEMIC

This year saw a 35% increase in attempted fraudulent transactions



PERCENTAGE OF FRAUD LOSS REPORTED BY AGE



WHAT INFORMATION RESONATES WITH YOU THAT YOU CAN TAKE INTO THE NEW YEAR?

SCAMMINGS PRESENT



20%
Claimed being
murdered as a
personal fear

72%
Of those
surveyed
indicated that
their greatest
fear was
having their
personal or
financial
information
stolen by
hackers

43%
Of
respondents
claimed
home
burglary as
a frequent
worry

There's no gift like the present.

And there's no anxiety like
identity theft.

According to a report on criminal
acts that people most feared, cyber
crimes made the top two worries
on the list.

67% Of survey-takers noted
becoming a victim of identity
theft as their main concern

It's hard to live
in the present
when worrying
about the future.

But knowledge is power!

Take advantage of any additional trainings
at your disposal. Find topics you have
concerns about or an interest in, and learn
some tactics to help you stay vigilant.

SCAM OF THE FUTURE (MONTH)

Steve is an up-and-coming scammer with a new scheme under his jingle-belt: he utilizes a real address (7 Smith Street) and a fake name (Max Grinchy) to open up real accounts and carry out transactions.

Lauren really lives on 7 Smith Street. She started receiving mail for Max Grinchy, but thought nothing of it, and threw the junk mail in the trash. Years later, she reviewed her credit report for the first time in a while, and noticed some activity that was not hers.

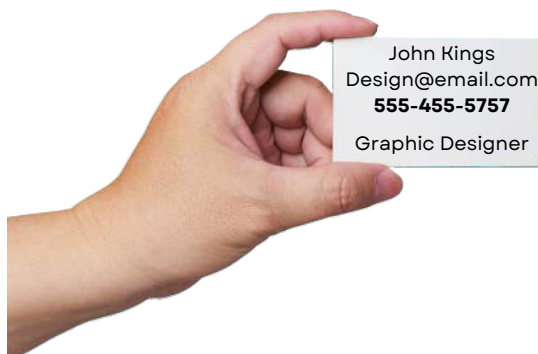
Synthetic Identity Fraud is the creation of a fictional persona, through the blending of stolen personal information with made-up details that fill in the gaps in order to open accounts and carry out transactions.

It's a relatively new process, and a fast growing financial crime method to be on the look out for.



Did you spot the red flags?

- ▶ Lauren suddenly started receiving mail to her address with someone else's name. This should have been a sign that her information was being mingled with other made up details to commit fraud.
- ▶ Lauren was not regularly checking her credit report. Had she been, she might have caught the suspicious activity much sooner.



In a Synthetic Identity Fraud case, though some of the information is made up, the parts that are real could be tied back to you and can have a negative impact.

Technically, there is no "victim" of Synthetic Identity Fraud, as the "person" exploited does not exist. Because of this, such crimes can go undetected for months.



Though Synthetic Identity Fraud can be difficult to detect and prevent, your best defenses are to use strong passwords, remain vigilant against phishing attempts, and regularly inspect personal accounts for suspicious activity.

Key Takeaways

The **past** holds a lot of cyber information that we can learn from to help us forge through the cyber-**present** with the courage needed to take on the **future**.

By reflecting on the past, learning as much as you can in the present, and staying on top of future trends, cybercriminals don't hold a snowflake to your cybersecurity awareness.



Review past cybercrimes. By learning where others went wrong, you can avoid making the same mistakes, catching on to cyber-patterns before they catch onto you.



Anxiety Society. If you fear your personal information being compromised, you're not alone. But don't let your worries consume you. Name them, learn more about them, and conquer them.

Reflection Section

Reflection allows for stillness amidst chaos, providing the space for the mind to interpret external stimuli and create deeper meaning.

How does this relate to cybersecurity?

It's a big cyber-world out there, with a lot of information. Some of it may not feel like it relates to you at first glance. But taking the time to look further, create connections, and observe will allow you to develop a strong cybersecurity mindset, which can then inform future actions.

Practice reflection.

Take the time to reflect on this newsletter, or on your next Micro Training. Consider these trainings from different angles to find key takeaways that create meaning within your own world.