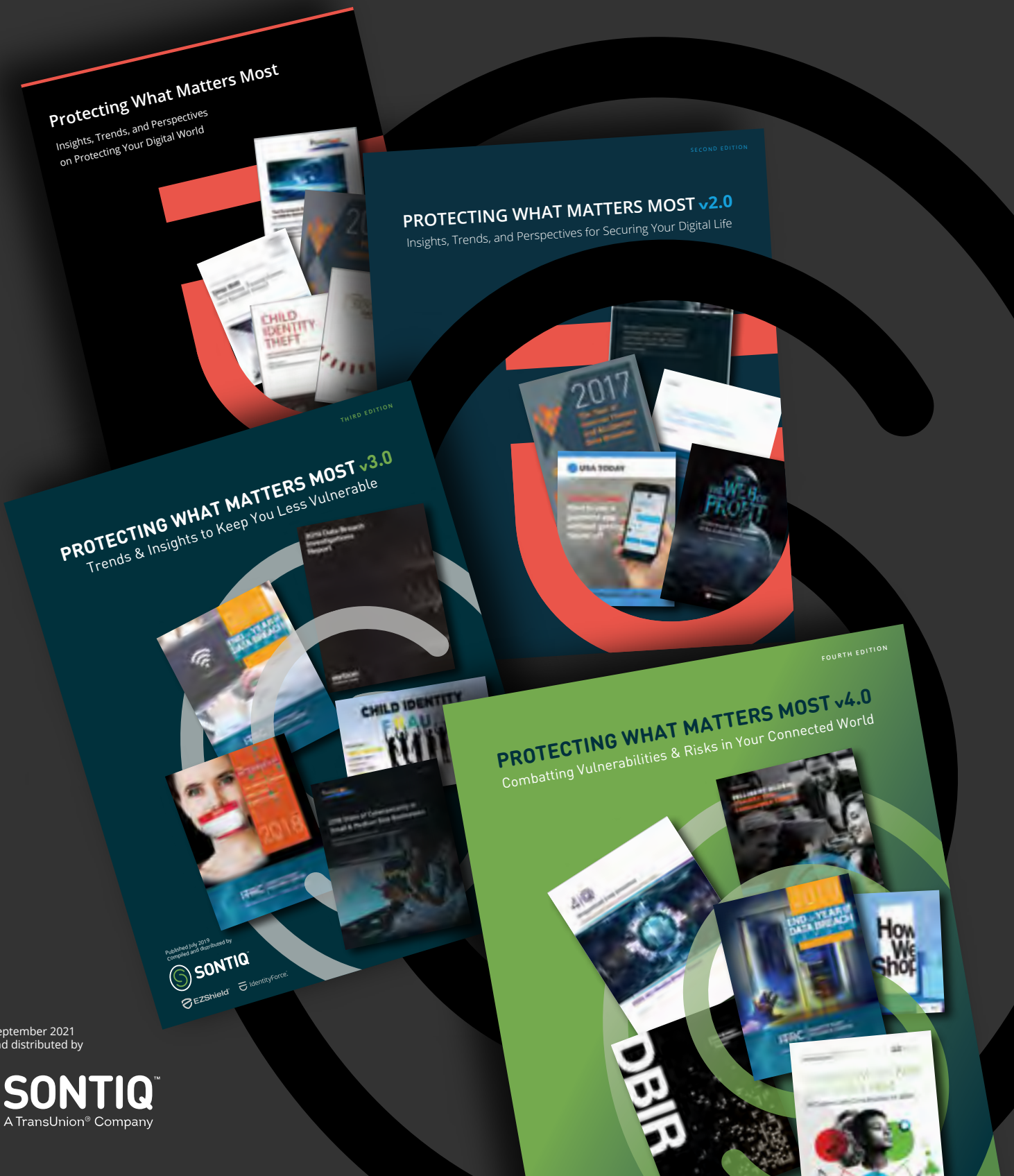
5 YEARS ANNIVERSARY EDITION

PROTECTING WHAT MATTERS MOST

Key Learnings & Tips to Protect YOUR Digital Safety & Security



Published September 2021
Compiled and distributed by

SONTIQ™
A TransUnion® Company

PARTY OF FIVE

We know consumers want to be empowered to protect themselves and everything they've built. They need to understand how data breaches and scams impact them directly in order to protect what matters most.

Access these top five resources today to learn more about protecting your digital safety and security:

1

ID TOOLKIT
Use the **Sontiq Intelligent Identity Security Toolkit** to help you better understand and protect against scams, fraud, and data breaches

2

TOP COVID-19 SCAMS
Quick reference **infographic** and **tip sheet** to defend against the COVID-19 scams popular with fraudsters

3

CONSUMER TIPS & EDUCATION
Stay current with the latest information on identity scams and fraud protection with the **IdentityForce Consumer Blog**

4

10 TIPS FOR BREACH VICTIMS
Download this **infographic** for recommended actions to take if your identity has been impacted by a data breach

5

PROTECTING CHILDREN AND FAMILIES
Discover **tips to safeguard children's Personally Identifiable Information** (PII) in the places where their personal information is most vulnerable.

5

A FIVE YEAR JOURNEY

ITRC
IDENTITY THEFT RESOURCE CENTER

Protecting yourself, your friends, family, and your workplace from identity crimes and compromises has become increasingly difficult. Fraudsters continue to exploit the health crisis, creating a "scamdemic." Identity thieves defraud our government systems to the tune of billions of dollars using the compromised identity credentials of unknowing victims. And, after several years of a downward trend, data breaches are on track to eclipse the astronomical numbers we witnessed in 2017.

All stakeholders have a role in reducing the effectiveness of threat actors who leverage our identities to commit fraud. Industry and government leaders must do their part, but individual consumers also have a role. You CAN reduce your risk by empowering yourself with knowledge and meaningful action steps. Helping consumers navigate this complex space and learn how to protect themselves takes a dedicated commitment from industry stakeholders. For the last five years, Sontiq has demonstrated this commitment by providing their ***Protecting What Matters Most*** e-book as a free resource to anyone who wants it.

Gaining control of your identity and reducing your risk can be a confusing and even scary undertaking. Taking advantage of free tools, though, is the first step to empowering yourself. This free e-book can help to lessen that confusion, enabling you to build a better understanding of where you are most vulnerable and — more importantly — what you can do about it.

Sincerely,

Eva Velasquez | *President/CEO* **at the Identity Theft Resource Center**

COVID AS CATALYST: FIVE YEARS OF CHANGE IN ONE

THE TOTAL IMPACT OF ID FRAUD

CONSUMER COST

Nearly **$600 MILLION** in COVID-Related Fraud

SOURCE | FTC COVID-19 Fraud and Stimulus Tracker

SEVERE EMOTIONAL DISTRESS

54% Report Feeling **VIOLATED**

SOURCE | ITRC 2021 Consumer Aftermath Report

LACK OF FUNDS

40% Unable to Pay **ROUTINE** Bills

SOURCE | ITRC 2021 Consumer Aftermath Report

COVID-19 has **compressed years of technical change** into one. Quick-turn innovation has given us flexibility but also impacted privacy and security at scale. And cybercriminals, who thrive in chaos, have capitalized on security weaknesses — from unemployment fraud to ransomware attacks against schools.

CYBER THREATS AT EVERY TURN

1 BUSINESS
The cost to businesses of an average data breach rose nearly 15% YoY in 2021. (Quartz)

2 EDUCATION
U.S. K-12 education systems experienced an 18% increase in reported cyberattacks in 2020 over 2019. (K12 Cybersecurity Resource Center)

3 HEALTHCARE
Nearly 1M people were affected by healthcare organization data breaches every month of 2020. (Wall Street Journal)

4 PUBLIC SAFETY
Hackers demanded $4M from Washington DC police to buy back more than 250GB of stolen data. (Forbes)

5 RETAIL
1 in 5 U.S. consumers have been the victim of online shopping fraud 2020–2021. (Riskified)

In 2020, **1.4 million consumers** reported identity fraud to the FTC, with $3.3 billion lost. In addition to financial and digital effects, there's an **intangible mental health impact** from the combined full-frontal assault of COVID-19 and cyberattacks.

Home should be our safe place. But the lines between private spaces and public lives continue to blur as we innovate for convenience. Shopping and in-person meetings have moved online, not always on secured networks. Unsurprisingly, online commerce was the **number one COVID-related fraud** between January 2020 and August 2021. In-office, behind-the-firewall work policies have been replaced by Bring Your Own Device (BYOD) interactions where the same phone that downloaded malware from a personal email is accessing company data. Even appliances in your kitchen are possible gateways to your family's personally identifiable information (PII) as the smart home becomes a reality. Preparing for these changes can help protect your identity and those of your family members.

TOP FIVE

Pandemic-Related Complaints Reported to State & Local Consumer Agencies in 2020

1. Price-gouging
2. Evictions
3. Business Closings
4. Canceled Events & Travel
5. Schools & Childcare

SOURCE | 2020 Consumer Complaint Survey Report

PARENT PERSPECTIVE

Sharon Vinderine *CEO and Founder*

parent tested parent approved™

FOUR STEPS FOR EFFECTIVE DIALOGUE ON DIGITAL RISKS

1) Talk to your children about what they are doing online and let them know you are watching.
Whether it's hidden usernames and accounts or limited answers, one of the most important things we can do to help our children is educate them. Teach them what is acceptable and not acceptable online.

2) Teach them about the "Pause and Post" rule.
My theory has always been to teach children that before they post something or send a private message, think about whether they would be comfortable with that message being shared on a huge billboard on a highway for everyone to see. *Even as adults, that is a rule to live by.*

3) There is no such thing as privacy on the internet.
There is an illusion that DMs or chats in Snapchat are private. But these are the types of messages that are most often shared and used as a form of cyberbullying. Screenshots of private messages have been known to spread faster than wildfire and cause incredible embarrassment and anxiety for kids.

4) Practice patience.
Take the time to listen and not lecture. Be creative in finding ways to connect with your children. Each child is a unique human with unique needs. Giving them the one-on-one attention they crave often offers an opportunity for them to open up to you. Do not miss out on that opportunity.

While social media apps like TikTok, Twitter, Snapchat, and Instagram have given children an opportunity to connect with their peers virtually, it has also exposed them to the dangers of the online world.

Since the pandemic, there has been:

A **70% increase in hate speech** between kids and teens during online chats.

A **40% increase in toxicity** on popular gaming platforms, such as Discord.

SOURCE | L1GHT Report: Rising Levels of Hate Speech & Online Toxicity During This Time of Crisis

Pre-COVID, most of our children had bedtimes, restrictions around how many hours they could be online, and more rules in place to keep them safe. We parents have been letting our guard down due to exhaustion from our own social isolation, our increased responsibilities in the home, and the impact of at-home schooling and virtual work environments. Bedtime and online time rules have been dropped because parents are concerned about children's isolation.

7 Signs of Cyberbullying

- Sudden decline in grades
- Withdrawal from family or friends
- Showing signs of depression or anxiety
- Significant changes in mood
- Changes in sleep habits
- Increasingly private when using phone, tablet, or computer
- Mood changes after receiving a text

What does this isolation mean for our children? How does living in a virtual world impact them? It has directly translated into a rise in the rate of anxiety, depression, and suicide. Some would say that this mental health crisis is its own pandemic.

DID YOU KNOW?

69% of U.S. teens say they use Snapchat.

Active Snapchatters open the app **30 times per day.**

18 billion videos are posted daily on Snapchat.

FIVE FRAUD FUTURES

FIVE WAYS TO PROTECT YOURSELF FROM CYBER FRAUD

1) **Public Wi-Fi.** To ensure information stays private, use a VPN to access company systems or sensitive files.

2) **Vishing.** Never give personal or financial information over the phone unless you initiated the call to a person or company you trust.

3) **Ransomware.** Invest in a high-quality cybersecurity solution that protects against malware attacks. Consider purchasing ransomware restoration protection.

4) **Software and system updates.** Download the latest patches and bug fixes and enable automatic updating.

5) **Education.** Learn to detect suspicious websites, malware, and spam. And use common sense. If anything offered online or over the phone seems too good to be true, it probably is.

Identity theft is a lifelong threat, but some identities are more prone to attack. Children fall into this category with over 1 million having their identity stolen annually. Recent data also shows that two-thirds of victims are 6 years old or younger. Child identity fraud can go undetected for many years, making our youngest population the most appealing to identity thieves.

1 MOBILE

Increased use of mobile devices has put individuals and organizations at risk of four main security threats: physical device, web-based, mobile network, and mobile app threats.

FIVE-YEAR EVOLUTION OF MOBILE THREATS

2017	2021
Improper Platform Usage 1	1 ..... Social Engineering
Insecure Data Storage 2	2 .... Data Leakage via Malicious Apps
Insecure Communication 3	3 ..... Unsecured Public Wi-Fi
Insecure Authentication 4	4 ..... End-to-End Encryption Gaps
Insufficient Cryptography 5	5 ..... Internet of Things (IoT) Devices

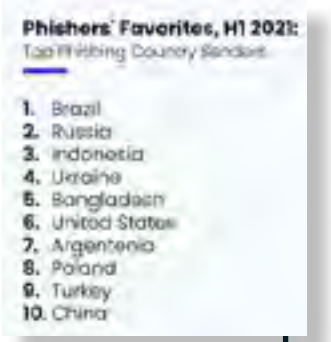
SOURCE | OWASP Mobile Security Top 10 Risks for 2017

SOURCE | 9 Most Common Security Threats to Mobile Devices in 2021

2 PHISHING

In phishing attacks, scammers send an email that appears to be from a trusted source and leads to a malicious link, malware download, and/or requests for personal information.

Q2 2021 saw a significant spike in phishing attacks (281%) in May and another 284% increase in June — totaling 4.2 billion phishing emails.



SOURCE | Phisher's Favorites Top 25 H1 2021, Worldwide Edition

3 OTHER SOCIAL ENGINEERING

Hackers also use SMS text messages (smishing) and phone calls/voicemail (vishing) to trick people into revealing private information or downloading malware.

Nearly 1 in 3 Americans have fallen victim to a phone scam in the past year.

4 RANSOMWARE

In ransomware attacks, cyber thieves freeze an organization's digital assets and exact a ransom to release them. Scammers use three primary tactics:

- **Scareware** pop-ups warn that malware has been detected and offer to remove it for a price.
- **Screen lockers** freeze users out of their PC and, upon reboot, present an official-looking message stating that illegal activity has been detected and that the user must pay a fine.
- **Encrypting ransomware** encrypts files and demands payment for unlocking and restoring them.

5 DATA BREACHES

In a data breach, sensitive, protected, or confidential information is exposed by hackers for personal gain. All sensitive personal information that is stored digitally is at risk.

In 2021, the global average total cost of a data breach is $4.2 million, up from $3.8 million in 2020.

A TALE OF TWO BREACHES

EXPERT PERSPECTIVE **Jim Van Dyke**

Jim Van Dyke is one of the country's foremost experts in data breaches. He was the co-founder of Breach Clarity, the founder of Javelin Strategy & Research, serves as a board member of the Identity Theft Resource Center, and is a former board member of the U.S. Consumer Financial Protection Bureau (CFPB/U.S. Treasury). Jim is currently SVP of Innovation at Sontiq.

SMBS UNDER FIRE

Big data breaches capture the headlines, but hackers have small and mid-size businesses firmly in their sights. The lack of large IT teams and comprehensive IT security programs make SMBs an attractive target for cyber thieves.

1 IN 5 small businesses fall victim to a cyberattack and of those, **60% go out of business in 6 MONTHS.**

SOURCE | Why Every Small Business Should Care About Cyberattacks, in 5 Charts

55% of SMBs have reported suffering a cyberattack

SOURCE | The State of SMB Cybersecurity 2020

ALMOST 1/3 of 2020's data breaches involved small businesses

SOURCE | 2020 Data Breach Investigations Report

46% of SMBs have been the targets of a ransomware attack and **73%** have paid a ransom

SOURCE | 2020 Infrascale Report

The average cost of a SMB data breach is **$2.63 MILLION**

SOURCE | 2021 Cost of a Data Breach

52% of SMBs agree they lack the in-house skills necessary to properly deal with security issues

SOURCE | The State of SMB Cybersecurity 2020

Following any breach, victims need to know specific threats to their personal identity and what actions best protect their financial health. That gives them the power to act quickly and effectively to mitigate risk.

Every breach raises a unique pattern of risks to identity-holders, depending on the particular identity credentials exposed. For example, a breach that exposes a Social Security number raises different risks for its victims than a breach that exposes payment card digits.

Let's contrast two recent breaches to illustrate how unique — and sometimes counterintuitive — identified identity risks can be from any of the thousands of breaches that occur each year. The following two breaches are comparable, having received a BreachIQ™ Breach Risk Score of 5 (out of 10 possible points). **However, the type of identity risks and the prescribed action steps to mitigate exposure can differ.**

NESHAMINY CONSTRUCTORS, INC.

November 2020
Attack type: Ransomware

Type of data stolen
- Social Security number
- Driver's license number
- Checking account numbers
- Credit card information
- Name

Primary risk
- Financial services account takeover
- New credit card account fraud

Actions victims should take
(in order of priority)
- Set up two-factor authentication at your bank or credit union
- Set fraud alerts on your credit report
- Set up credit report monitoring
- Lock or freeze your credit report

AmeriCommerce

April 2021
Attack type: Ecommerce website compromise (Magecart)

Type of data stolen
- Payment card information
- Email address
- Physical home address

Primary risk
- Payment card fraud
- Email-based crime (eg. phishing)

Actions victims should take
(in order of priority)
- Set alerts for your credit and debit card accounts and monitor regularly
- Set alerts for or lock online card transactions
- Set up criminal marketplace scanning
- Set alerts and monitor for suspicious activity on your email account

BreachIQ's proprietary algorithm uses artificial intelligence to analyze 1,300+ data points to assess the risks of a data breach. It detects when a data breach has compromised an individual's personal data on the Dark Web, determines what specific information has been impacted, and curates custom risk mitigation strategies.

Consumers affected by any data breach need to be on heightened alert for outreach from identity criminals, including phishing and vishing. Fraudsters will attempt to use information exposed in a previous data breach — correct names, account numbers, Social Security numbers — to trick you into divulging more sensitive data, downloading malware, or giving access to secured areas.

THE FUTURE OF IDENTITY RISK

EXPERT PERSPECTIVE **Al Pascual**

A recognized expert on cybercrime, Al Pascual co-founded Breach Clarity, led Javelin Strategy & Research, and served as their head of the Fraud & Security practice, where he directed the company's oft-cited research and analysis on consumer identity theft trends. Al is currently SVP, Data Breach Solutions at Sontiq.

CHECK FIVE ACTION PLAN

There are steps you can take NOW to mitigate future fraud:

- ☑ **NEW ACCOUNT FRAUD:** Monitor your identity for breaches that put you at higher risk, as well as new bank accounts or credit products obtained in your name.
- ☑ **DIGITAL IDENTIFICATION:** Continue to monitor the breadth of your identity health, especially the security of sensitive personal information, like your driver's license number, to prevent and detect any potential misuse.
- ☑ **GET AWAY FRAUD:** Be wary of unsolicited offers for large travel or electronics purchases that play into your desire to escape – especially from brands you haven't done business with. Pursue offers separately from the emails, texts, or calls you receive (i.e., never complete a transaction through a link or phone number sent to you with the offer).
- ☑ **MINOR MULES:** Before opening your child's bank account, educate them on scams. After their account is open, sign up for account alerts to quickly detect unexpected account activity and watch for large deposits and withdrawals.
- ☑ **EMPLOYMENT IMPERSONATION FRAUD:** Use a strong LinkedIn password and two-factor authentication. Don't add unfamiliar contacts or respond to unsolicited requests for information. Check your credit report regularly for unexpected new employers.

By knowing where fraudsters perceive the most opportunity in the next five years, consumers can take proactive steps to keep themselves and their families safe.

1. **NEW ACCOUNT FRAUD WILL EXPLODE.** Criminals open new accounts using stolen identities to obtain loans, move illicit funds, and more. New fraudsters who have honed their skills on government benefits fraud (e.g., state unemployment and Paycheck Protection Program [PPP]) are in a good position to transfer their skills to other targets, like financial institutions, credit card issuers, and lenders.

2. **DIGITAL DRIVER'S LICENSES WON'T BE A PANACEA.** State-issued identity cards (e.g., driver's licenses) are going digital, so you'll store and present the ID right on your phone. Banks and merchants will likely take a long while to accept these new digital IDs the 'right way' — opening the door to abuse. And centralized databases of digital ID data will make enticing breach targets.

At least 17 states have considered or implemented digital driver's licenses

SOURCE | Digital Driver's Licenses Gaining Momentum Amid Pandemic

3. **YOUR NEXT VACATION MAY TAKE YOU FOR A RIDE.** Scams will become a major brand headache for travel and technology companies and the consumers fooled by them.

4. **MULE COLTS. YES, MULE COLTS.** Banking for kids will become increasingly common, making them targets for fraudsters looking for unwitting partners. These fraudsters solicit bank account holders to help move stolen funds under false pretenses — turning them into money mules — for a small piece of the action. Children are left to take the heat for illicit transfers.

30% of all money mules are under 21

SOURCE | Under 21s Recruited as Money Mules More Than Triple

5. **FRAUDSTERS WILL GET JOBS, SORT OF.** Employment impersonation fraud — where criminals pose as legitimate applicants — will take off as more employers keep remote roles. Criminals can glean information from professional networking and recruiting sites, like LinkedIn or even take them over to assume your identity. And armed with a convincing resume — plus all the compromised data they need to pass a background check — these newly hired 'employees' steal company secrets, compromise financial accounts, and possibly deliver ransomware.

TIPS FOR THE NEW NORMAL

FROM EQUIFAX TO NOW

5 Years of Big Breaches

2017 | Equifax

148 million records including Social Security numbers, credit/debit card information, driver's licenses, names, birth dates, and physical addresses.

2018 | Apollo

200 million records including job titles, employers, social media handles, phone numbers, email addresses, and business contact information.

2019 | Verifications.io

982 million email accounts, paired names, gender, dates of birth, employers, and home addresses.

2020 | Instagram | TikTok | YouTube

235 million user profiles including names, ages, genders, profile photos, account descriptions, and statistics about follower engagement and demographic.

2021 | Facebook | LinkedIn

533 million Facebook user records and 500 million LinkedIn user profiles including names, emails, addresses,phone numbers, account IDs, locations, birth dates, professional titles, and other work-related personal data.

Over the last five years, privacy and security have often been trade-offs for speed and convenience. The *new normal* for the next five years will be more convenient, more remote, and more digital, with more PII online across every demographic.

YOUNG AND OLD ARE VULNERABLE TO FRAUD

CHILDREN are **51X** more likely to be victims of identity theft than **ADULTS**.

SOURCE | Child Identity Theft

Online scams against **PEOPLE UNDER 21** have increased **156%** in the last three years.

SOURCE | State of Internet Scams 2021

In 2020, **SENIOR CITIZENS** lost almost **$1 billion** to scams.

SOURCE | Elder Fraud Report 2020

The uptick in cyber threats has been a global wake-up call to consumers, businesses, and governments. And lawmakers and regulators are getting involved. In the U.S., President Biden called a CEO Summit in the wake of infrastructure supply chain attacks, including the Colonial Pipeline ransomware attack, calling cybersecurity a "core national security challenge."

What can individual consumers and families do with a cybercrime problem so vast that Big Tech is pledging millions to battle it? Plenty!

In the big picture, hackers aren't stealing people's highly secured data by cunningly breaking the technological barriers of big companies. Everyday people are giving them the keys. Phishing accounts for 90% of data breaches, demonstrating that people are helping hackers access their personal data without realizing it.

Identity fraud cost Americans ~$56 billion in 2020. $43 billion was attributed to ID theft scams where criminals interact directly with consumers (e.g. robocalls and phishing emails), stealing the victim's information.

SOURCE | 2020 Identity Fraud Study

You can shut down opportunistic hackers with these three simple actions:

- **Inventory your passwords.** It may sound counter-intuitive but start with passwords to the things you no longer use (devices, computers, old email addresses, networks). Chances are, you're smarter today about password security than you were 2, 5, 10 years ago.
- **Call the local unemployment office.** COVID-19 unemployment fraud is estimated to be up to $400 billion. Red flags for benefits fraud are very subtle. Call in and ask if anyone has filed a claim using your name, address, or SSN.
- **Lock down your home-based IoT.** The connected home puts private data at risk and makes your home a prime entryway for hackers — to your data and your employer's. Device spoofing is on the rise. The first step is to opt out of Amazon Sidewalk. If you haven't yet, your home Wi-Fi is probably being shared.

DIVE DEEPER TO LEARN MORE

AARP

Top Scams Targeting Older Americans

https://www.aarp.org/money/scams-fraud/info-2021/schemes-targeting-older-adults.html

APRIORIT

OWASP Mobile Security: Top 10 Risks for 2017

https://www.apriorit.com/dev-blog/435-owasp-mobile-top-10-2017

AUTH0

The 9 Most Common Security Threats to Mobile Devices in 2021

https://auth0.com/blog/the-9-most-common-security-threats-to-mobile-devices-in-2021/

BARCLAYS

Under-21s Recruited As 'Money Mules' More Than Triple, Barclays Warns University Students

https://home.barclays/news/press-releases/2020/09/under-21s-recruited-as--money-mules--more-than-triple--barclays-0/

BLOOMBERG LAW

Kasaya Software Hack Highlights Small Business Security Squeeze

https://news.bloomberglaw.com/privacy-and-data-security/kaseya-software-hack-highlights-small-business-security-squeeze

BUSINESS LIVE

Warning as Barclays Says Third of Money Mules are Under 21

https://www.business-live.co.uk/enterprise/warning-barclays-says-third-money-16943319

CARNEGIE MELLON CYLAB

Child Identity Theft

https://www.cylab.cmu.edu/_files/pdfs/reports/2011/child-identity-theft.pdf

CNBC

Coronavirus Pandemic Turbocharges Online Sales

https://www.cnbc.com/2020/08/18/e-commerce-sales-grew-more-than-30percent-between-q1-and-q2.html

Biden Signs Executive Order to Strengthen Cybersecurity After Colonial Pipeline Hack

https://www.cnbc.com/2021/05/12/biden-signs-executive-order-to-strengthen-cybersecurity-after-colonial-pipeline-hack

CSO

Amazon Sidewalk Highlights Network Security Visibility Risks Consumer Services Pose

https://www.csoonline.com/article/3629439/amazon-sidewalk-highlights-network-security-visibility-risks-consumer-services-pose.html

CARING FOR KIDS

Social Media: What Parents Should Know

https://www.caringforkids.cps.ca/handouts/behavior-and-development/social_media

CISCO

2021 Cyber Security Threat Trends

https://umbrella.cisco.com/info/2021-cyber-security-threat-trends-phishing-crypto-top-the-list

Go Phish: Avoid Being Hooked by Phishing Emails

https://umbrella.cisco.com/blog/go-phish-avoid-being-hooked-by-phishing-emails

CONNECTWISE

The State of SMB Cybersecurity 2020

https://www.connectwise.com/globalassets/media/assets/ebook/the-state-of-smb-cybersecurity-2020.pdf

CONSUMER FEDERATION OF AMERICA
2020 Consumer Complaint Survey Report
https://consumerfed.org/wp-content/uploads/2021/07/Top-2020-Consumer-Complaints-Report.pdf

FEDERAL BUREAU OF INVESTIGATION
2020 Elder Fraud Report
https://www.ic3.gov/Media/PDF/AnnualReport/2020_IC3ElderFraudReport.pdf

FEDERAL TRADE COMMISSION
Equifax Data Breach Settlement
https://www.ftc.gov/enforcement/cases-proceedings/refunds/equifax-data-breach-settlement
Fraud Loss to COVID-19
https://public.tableau.com/profile/federal.trade.commission#!/vizhome/COVID-19andStimulusReports/Map
New Data Shows FTC Received 2.2 Million Fraud Reports from Consumers in 2020
https://www.ftc.gov/news-events/press-releases/2021/02/new-data-shows-ftc-received-2-2-million-fraud-reports-consumers
The Top Frauds of 2020
https://www.consumer.ftc.gov/blog/2021/02/top-frauds-2020

FINANCIAL TIMES
Big Tech Groups Make Cyber Security Pledges After White House Summit
https://www.ft.com/content/f6fa1f66-6a26-4ae0-b5a2-560c887b1998

FORBES
Ransomware Hackers Claim to Leak 250GB of Washington, DC, Police Data After Cops Don't Pay $4 Million Ransom
https://www.forbes.com/sites/thomasbrewster/2021/05/13/ransomware-hackers-claim-to-leak-250gb-of-washington-dc-police-data-after-cops-dont-pay-4-million-ransom

FORTUNE
More Than 1 Million Children Were Victims of Identity Theft in 2017
https://fortune.com/2018/04/24/stolen-identity-theft-children-kids/

FOX
Digital Driver's Licenses Pandemic Gaining Momentum Amid Pandemic
https://www.fox43.com/article/tech/digital-drivers-licenses-pandemic/521-11b77910-f65e-46b4-b480-a6305f4b1831

HELPNETSECURITY
Houdini Malware Returns, Enterprise Risk Assessment Compromised By Amazon Sidewalk
https://www.helpnetsecurity.com/2021/08/18/houdini-malware/

IBM
Cost of a Data Breach Report 2021
https://www.ibm.com/security/data-breach

IDENTITY THEFT RESOURCE CENTER
2020 Annual Data Breach Report
https://notified.idtheftcenter.org/s/2020-data-breach-report

INFRASCALE
2020 Infrascale Report
https://www.infrascale.com/press-release/new-infrascale-research-indicates-more-than-1-in-5-smbs-lacks-proper-data-protection/

JAVELIN
2020 Identity Fraud Study: Genesis of the Identity Fraud Crisis
https://www.javelinstrategy.com/press-release/identity-fraud-losses-increase-15-percent-consumer-out-pocket-costs-more-double

K-12 CYBERSECURITY RESOURCE CENTER AND THE K12 SECURITY INFORMATION EXCHANGE
The State of K-12 Cybersecurity: 2020 Year in Review
https://k12cybersecure.com/wp-content/uploads/2021/03/StateofK12Cybersecurity-2020.pdf

L1GHT REPORT
Toxicity During Coronavirus
https://l1ght.com/Toxicity_during_coronavirus_Report-L1ght.pdf?fbclid=IwAR12yPh-Gli1Ur1qwwZoCuu4nP2zG5dLxs590Exli5UXYORQCWp3w_ko1MQ

NEWS MEDICAL
The Impact of COVID-19 on Mental Health and Family Finances
https://www.news-medical.net/news/20210824/The-impact-of-COVID-19-on-mental-health-and-family-finances.aspx

MCKINSEY
How COVID-19 Has Pushed Companies Over the Technology Tipping Point
https://www.mckinsey.com/business-functions/strategy-and-corporate-finance/our-insights/how-covid-19-has-pushed-companies-over-the-technology-tipping-point-and-transformed-business-forever

MIMECAST
The State of Email Security 2020
https://www.mimecast.com/state-of-email-security/

NEWS-MEDICAL.NET
The Impact Of Covid-19 On Mental Health And Family Finances
https://www.news-medical.net/news/20210824/The-impact-of-COVID-19-on-mental-health-and-family-finances.aspx

NBC NEWS
'Easy Money': How International Scam Artists Pulled Off An Epic Theft Of Covid Benefits
https://www.nbcnews.com/news/us-news/easy-money-how-international-scam-artists-pulled-epic-theft-covid-n1276789

NCBI
Impact of Social Isolation and Loneliness on the Mental Health of Children & Adolescents
https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7267797/

NATIONAL CENTER FOR BIOTECHNOLOGY INFORMATION (NCBI)
Rapid Systematic Review: The Impact of Social Isolation and Loneliness on the Mental Health of Children and Adolescents in the Context of COVID-19
https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7267797/

OMNICORE
Snapchat by the Numbers: Stats, Demographics & Fun Facts
https://www.omnicoreagency.com/snapchat-statistics/

PONEMON INSTITUTE
Cybersecurity in the Remote Work Era
https://www.keepersecurity.com/ponemon2020.html

PEW RESEARCH CENTER
10 Facts About Americans And Facebook
https://www.pewresearch.org/fact-tank/2021/06/01/facts-about-americans-and-facebook/

PREY PROJECT
Mobile Theft & Loss Report 2020
https://preyproject.com/uploads/2020/03/Mobile-Theft-Loss-Report_2020.pdf

RISKIFIED
A Crisis of Confidence
https://www.riskified.com/content-hub/ecommerce/econfidence-guide

SOCIAL CATFISH
State of Internet Scams 2021
https://socialcatfish.com/blog/state-of-internet-scams-2021/

SONIC
2021 Mid-Year Update Sonicwall Cyber Threat Report
https://www.sonicwall.com/2021-cyber-threat-report/

TECHCRUNCH
Snapchat Beats In Q3, Adding 7m Users & Revenue Up 50%
https://techcrunch.com/2019/10/22/snapchat-earnings-q3-2019/

TECH REPUBLIC
COVID-19 Emergence Leads to 37% Jump in Mobile Phishing Attacks in 2020
https://www.techrepublic.com/article/covid-19-emergence-leads-to-37-jump-in-mobile-phishing-attacks-in-2020/

TRUECALLER
Spam & Scam Report 2021
https://truecaller.blog/2021/06/28/us-spam-scam-report-21/

U.S. DEPARTMENT OF HEALTH AND HUMAN SERVICES
Fraud Alert: COVID-19 Scams
https://oig.hhs.gov/fraud/consumer-alerts/fraud-alert-covid-19-scams

U.S. SMALL BUSINESS ADMINISTRATION
2020 Small Business Profile
https://cdn.advocacy.sba.gov/wp-content/uploads/2020/06/04144224/2020-Small-Business-Economic-Profile-US.pdf

VERIZON
2021 Data Breach Investigations Report
https://www.verizon.com/business/resources/reports/dbir/

VADE
Phishers' Favorites Top 25 H1 2021, Worldwide Edition
https://www.vadesecure.com/en/blog/phishers-favorites-top-25-h1-2021-worldwide-edition

VOX
Why Every Small Business Should Care About Cyberattacks, In 5 Charts
https://www.vox.com/sponsored/11196054/why-every-small-business-should-care-about-cyber-attacks-in-5-charts

THE WALL STREET JOURNAL
Hospitals Suffer New Wave of Hacking Attempts
https://www.wsj.com/articles/hospitals-suffer-new-wave-of-hacking-attempts-11612261802?mod=tech_lead_pos13

Biden Says Cybersecurity Is the 'Core National Security Challenge' at CEO Summit
https://www.wsj.com/articles/biden-to-hold-cybersecurity-summit-with-tech-giants-top-banks-energy-firms-11629882002

THE WHITE HOUSE
FACT SHEET: Biden Administration and Private Sector Leaders Announce Ambitious Initiatives to Bolster the Nation's Cybersecurity
https://www.whitehouse.gov/briefing-room/statements-releases/2021/08/25/fact-sheet-biden-administration-and-private-sector-leaders-announce-ambitious-initiatives-to-bolster-the-nations-cybersecurity/

QUARTZ
Why The Cost Of Getting Hacked Is Higher Than Ever
https://qz.com/2039599/why-the-cost-of-getting-hacked-is-higher-than-ever/

ZDNET
After a Breach, Users Rarely Change Their Passwords, Study Finds
https://www.zdnet.com/article/after-a-breach-users-rarely-change-their-passwords-study-finds/

“IN TODAY’S WORLD, IT’S NO LONGER A MATTER OF ‘IF’ YOUR PII IS BREACHED. INSTEAD, THE QUESTION HAS QUICKLY BECOME **‘HOW MANY TIMES’ HAS YOUR PII BEEN BREACHED.** AS A RESULT, IDENTITY PROTECTION SERVICES OFFER PERSONAL PEACE OF MIND AND PROACTIVE SOLUTIONS TO HELP OUR CUSTOMERS STAY ONE STEP AHEAD.”

MIKE MEYER, *Retail Product Manager*

Commerce Bank

“WHILE THE AMERICAN PUBLIC WAS FOCUSED ON PROTECTING OUR FAMILIES FROM A GLOBAL PANDEMIC AND HELPING OTHERS IN NEED, **CYBER CRIMINALS TOOK ADVANTAGE OF AN OPPORTUNITY TO PROFIT FROM OUR DEPENDENCE ON TECHNOLOGY** TO GO ON AN INTERNET CRIME SPREE.”

2020 Internet Crime Report (released by the FBI’s Internet Crime Complaint Center)

ABOUT SONTIQ

Sontiq, a TransUnion company, is an intelligent identity security company arming businesses and consumers with a full range of award-winning identity and cyber monitoring solutions, as well as best-in-class restoration and response offerings. Sontiq products empower millions of customers and organizations to be less vulnerable to the financial and emotional consequences of identity theft and cybercrimes. Sontiq has an outstanding track record for delivering high-touch support and fraud remediation services, demonstrated through its 99% customer satisfaction ratings.
https://www.sontiq.com