SONATA BANK FINANCIAL WELLNESS SERIES

How You Can Stay Safe From Cyber Threats in 2024 & 2025

sonata bank

IMPORTANT DISCLOSURE

Before We Begin

The information provided in this eBook, “HOW YOU CAN STAY SAFE FROM CYBER THREATS IN 2024 & 2025,” is for general informational and educational purposes only. While we strive to keep the information up-to-date and correct, we make no representations or warranties of any kind, express or implied, about the completeness, accuracy, reliability, suitability, or availability of the information contained in this eBook for any purpose.

This eBook is not intended as a substitute for professional advice. The field of cybersecurity is complex and constantly evolving, and individual situations can vary greatly. Therefore, we strongly recommend that readers consult with qualified cybersecurity experts or legal advisors for personalized guidance tailored to their specific circumstances.

Any reliance you place on the information in this eBook is strictly at your own risk. We will not be liable for any loss or damage arising from the use of any information contained within this publication.

Please note that cybersecurity laws, regulations, and best practices may change over time. It is the reader’s responsibility to stay informed about current developments in cybersecurity and to comply with all applicable laws and regulations.

By reading and using this eBook, you acknowledge that you have read and understood this disclosure statement.

INTRODUCTION

Recent Cybersecurity Breaches have Brought Attention to the Growing Threat We All Face

In April of 2024, millions of Americans' Social Security numbers were stolen by the hacking group "USDoD" in one of the largest breaches in history. These hackers stole 2.9 billion personal records from NationalPublicData.com, a company that collects and aggregates public records. This data includes sensitive personal information like home addresses, Social Security numbers, and private phone numbers.

Even if the USDoD hackers didn't exist, statistically, one in three Americans* have already had our identities stolen. That statistic will surely rise, thanks to the recent theft. According to MyFICO,* your FICO credit score drops an average of five points when your identity is stolen. If you're trying to apply for a mortgage or loan and your FICO score is right on the border of being accepted, this credit score drop could have major implications on your financial plans.

Having this threat hanging over our heads is unsettling. To that end, Sonata Bank has written this eBook in simple, straightforward language to protect you from becoming the victim of identity theft. This eBook also serves to help you know your rights if you experience a cybersecurity breach, and to help you prepare for the best possible outcome if — or when — it happens.

CHAPTER ONE

Common Threats and Scams You Need to Know About Now

The average, law-abiding citizen would never consider the threats that are now lurking everywhere. Free “guest” wi-fi at the local coffee shop or hospital waiting room can set you up for identity theft if you don’t have anti-spyware protection on your phone or laptop computer to cloak your personal data. Another culprit most people would never consider being an identity theft vulnerability is your rental car. When you pair your phone to use your rental car’s navigation system, your personal data is also connected. It will remain connected for the next car rental driver, **unless you proactively remove it**.

The most common threats are “phishing emails,” which are escalating in their frequency and sophistication levels. You’ve probably noticed you’re getting fewer old-school Nigerian prince emails. The infamous Nigerian prince scam sought your bank account details so this supposed random prince could deposit his money into your bank account for safekeeping until he could escape whatever country he claimed to be held captive in.

Today, free A.I. programs like ChatGPT are helping the cyber criminals (most for whom English is a second language) to improve their grammar and punctuation. Thanks to A.I., they can email you “phishing attack” emails that sound like an American wrote them as they ask for your personal details.

Let’s review some of the more commonplace email scams people are experiencing today.

THE “YOU HAVE A PACKAGE” SCAM:

One of the delivery companies (Amazon, FedEx, DHL, or UPS) will send you a fake email stating, “We cannot deliver this item without more information. Please click here to confirm your delivery information.” Once you click on the link they provide, it will send you to a fake website where they ask for your address, phone number, or other personal information to build your profile so they can complete their identity theft.

THE “THIS INVOICE WILL DRAW FROM YOUR BANK ACCOUNT ON THIS DATE” SCAM:

You’ll receive an invoice emailed as a PDF attachment for a sizable dollar figure. The email will warn you that this amount is about to be withdrawn from your bank account on a near-future date. If you click on the PDF to see what the invoice is, this is how a trojan horse virus will get embedded onto your computer so hackers can access your information.

THE "YOUR EMAIL ACCOUNT WILL BE CLOSED" SCAM:

Here is an example of the email scam recently sent from a fake "Yahoo" administrator:

Dear Email User,

Important! The old version mailbox closure notification mail below was sent to you not long ago and it wasn't treated as required. We are hereby calling your full attention to it again.

Please click the button below to Re-login and Confirm your email address now.

CONFIRM YOUR EMAIL

Warning: Your email account will be closed if not updated as it will be assumed as no longer in use.

Yahoo Mail Team

Never click links or download attachments unless you are certain the sender is safe.

You can confirm the sender's email address or a linked web address by hovering over the address with your cursor. Scammers will try to trick you by hiding the true email or web address.

THE "YOUR CREDIT SCORE HAS CHANGED" SCAM:

We're all protective of our credit scores, and services like CreditKarma, Transunion, or Experian frequently email us with credit score updates or changes. Sometimes these emails come more than once a day, so it is not unusual to receive an email like this. **Do not click** on these emails. Instead, download these services' apps to your phone and check for any credit score changes via your apps.

THE "HELP! I'M STRANDED AND NEED MONEY SEND ASAP" SCAM:

Another familiar scam is to receive an email from someone who pretends to be your CEO, friend, or family member who has been robbed and lost their wallet. As the scam goes, the story is always that they are supposedly stranded somewhere far away without access to money. Often these emails will state that the person is out of the country, or even in jail. The hackers watch people's social posts to see when they're traveling out of the state or country, which makes these email requests sound even more convincing. Never fall for this scam, even if you receive a phone call and hear that person's voice on the phone. That, too, can be faked.

How A.I. has Made These Scams More Convincing

These phishing scams have gotten much more sophisticated. A.I. has given cyber criminals a new and improved tool to convince people their emailed money requests are authentic: **deep fakes**. You may recall the recent news story about the grandmother who received a phone call with her grandchild's voice at the other end stating they were in danger and needed emergency money. Criminals need just three seconds of someone's speaking voice audio to create a voice print of (or audio copy of) that voice to then use it to make an audio recording with their money demands. Criminals can use A.I. programs like Descript.io to convert someone's still image into a video recording of that person. They can also convert your video into other languages, even matching your lip movements to the audio in foreign languages.

CHAPTER 2

How To Combat Emerging Cyber Threats

For many of us, the genie is already out of the bottle. We're all vulnerable to personal identity theft. Most of us have still images of ourselves online, even if it's an innocent Linkedin profile image. Someone can use that picture to create a deep fake video. Even if you are not an influencer or active on social media, the "new normal" is to live life like we're all in a reality TV show, posting every travel image, restaurant meal, and personal moment online. Unfortunately, this creates a wealth of material for cyber criminals to exploit to their advantage.

How can you protect yourself? Here are some best practices:

How to Know if an Email is a Scam: Most shipping companies will send you an email confirmation for your shipment, but they will not ask you for your personal information. Amazon, for example, will send you an email confirming that your package is on its way, and then send a follow-up email with a photograph of your package wherever the delivery person left it. **Always check the email address of the email**. It will typically be someone's personal gmail account or some random email address that is completely different from the shipper's email.

How to Know if a Website is Safe: Always look for the prefix https:// at the front end of the URL for the website you are visiting. This URL protocol means that your data is encrypted in both directions, coming to and from the server. When the “s” is absent, you are not on a safe site and malicious parties can see what data is being sent.

How to Prevent Rental Car Personal Data Theft: When you are ready to return your rental car, make it your habit to always perform the following protocol to ensure the next person renting your car doesn’t have access to your personal data:

1. Navigate to the settings section of your vehicle’s infotainment or multimedia system.
2. Look for an option that pertains to personal data, settings, or a factory reset.
3. Choose the reset or delete option. Some systems may call it ‘clear personal data,’ ‘factory reset,’ or ‘restore default settings.

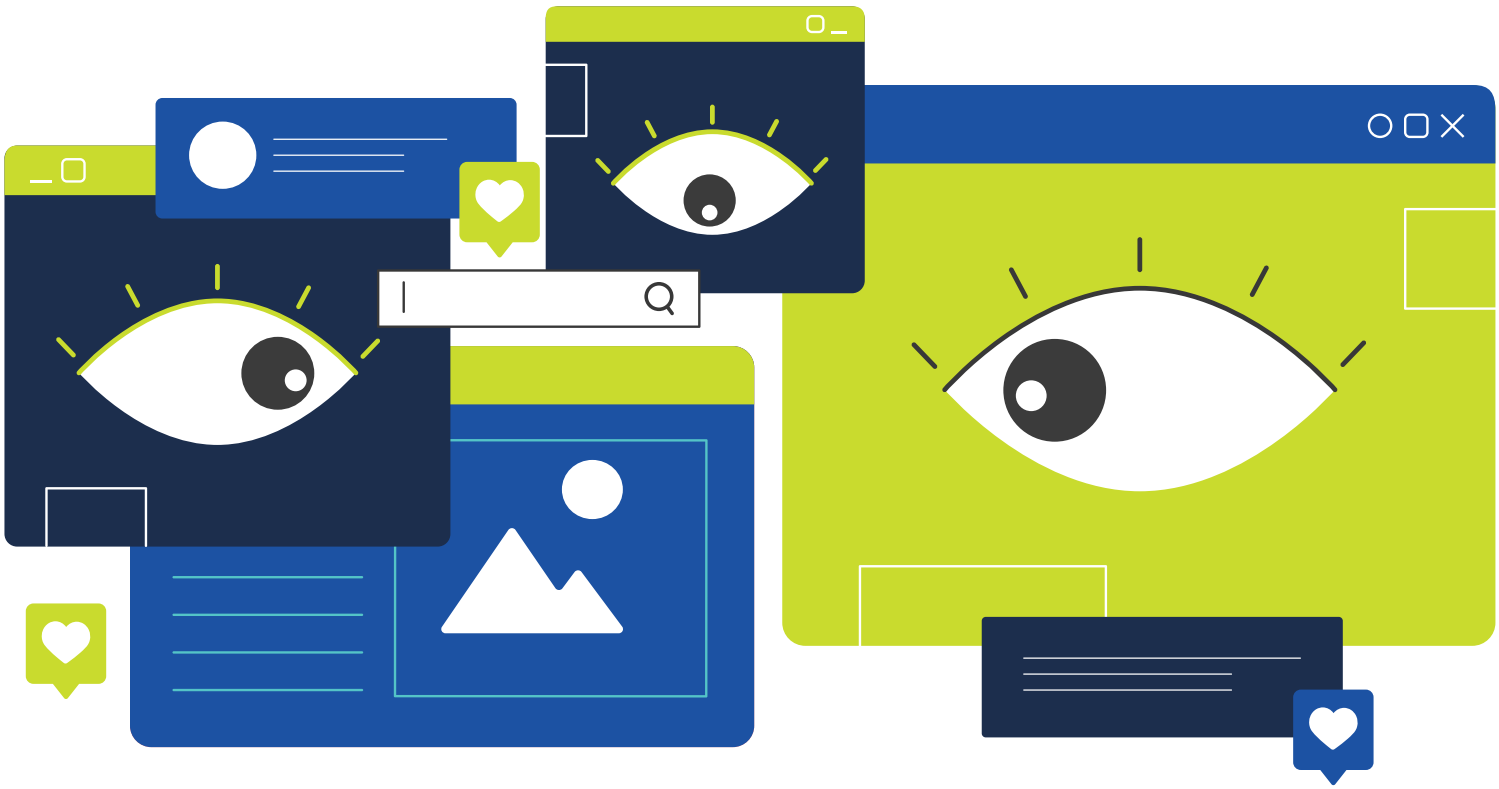
How to Prevent "Emergency Funds Transfer" Scams: Set up a code word with your loved ones or co-workers so no one believes or responds to scammers unless you or they state the predetermined code word. Make it your automatic protocol to hang up and call the person calling with urgent need of money to verify it's legitimate.

How to Raise Your Malware-ness: Never click on a link or attachment from a strange email address. Ever. If you do and it's from a hacker, this gives cyber criminals the trojan horse into your computer, access to all of your personal data, and the ability to spread viruses out to anyone you've ever communicated with on your email account. Avoid clicking on websites that do not have https:// (the "s" stands for "secure").

How to Delete Your Digital Breadcrumbs: Personal Data Removal Services — There are 200+ data broker sites out there, which triggered the creation of subscription-based services like DeleteMe* and Optery*, which proactively remove your data from sites like Spokeo, Intelius, Checkmate, and PeopleFinder. You can do this yourself, but with so many data brokers out there, it's time consuming.

How to Get the Most Out of Your Anti-Spyware Software: Here is a recent 2024 list* of the top-rated anti-spyware software to install on your system for the best protection. Once you install anti-virus protection software, you will receive alerts when it is time to update your virus protection. Be sure to do so as soon as possible, because the criminals are working nonstop to program viruses to attack the holes in your software and gain access to your computer.

How to Protect Yourself on Social Media: Set your privacy settings so that you only allow the people who *know you* to see your posts and photos. Do not post your plans for future trips or dates you're going to be out of town or out of the country. If you have elderly relatives, set their privacy settings for their own protection. Do not let them accept "friend requests" without vetting them thoroughly first.



How to Search for Your Own Images Theft: There are many apps* that can perform a "reverse image search" to identify if fake images or footage of you exist online. To get alerted any time your name is mentioned online, you can set up Google.com/alerts for free to perform "social listening."

To set up a Google alert, do the following:

1. **On your browser, simply enter https://www.google.com/alerts***
2. **Enter the search query that you want to monitor.** You will see an overview of the types of results you will receive beneath the search box. If the results don't look exactly like what you want, put quote marks around your name so you receive that exact wording and spelling in your Google Alert.
3. **Select your desired source.** Click the *More options* link beneath the search box. Then, click the dropdown menu to the right of ***Source***. You can choose as many options as you would like to include by clicking. A checkmark will appear by selected sources.

Automatic: Will show you the results that contain the best results, regardless of the source.

Blogs: Will only return results from blogs. Blogs aren't always the best way to get the most reliable information, but it will help if you want to gauge the feeling that the online community has toward a subject.

News: Will return results from sites such as the New York Times and the Washington Post. This is a good source to include if you are monitoring an ongoing event or story.

Web: Will deliver results from all across the web, such as forums and other online communities.

Video: Will return video results.

4. **Choose how often you wish to receive the alert.** Click the *More options* link beneath the search box. Then, click the dropdown menu to the right of ***How often***. We recommend you choose "***As-it-happens***."

As-it-happens: Google will send alerts to your e-mail with new content related to your search term right as it happens. This is extremely useful if you need to receive up-to-date news on a continuing story or event. However, it will result in a large number of e-mails.

At most once a day: Google will send you an alert with a summary of new content related to your search term once a day. If your search term is fairly obscure and not much is happening with it, you may not receive an alert on some days.

At most once a week: Google will send you an alert with a summary of new content related to your search term once a week. This is a good option if your search term is somewhat obscure and new information on it is not released frequently.

5. **Choose between "All results" and "Only the best results."** Click the *More options* link beneath the search box. Then, click the dropdown menu to the right of ***How many***. If you choose ***All results***, you will receive any new information related to the search term even if the information is of low-quality.

6. **Choose the region.** Click the *More options* link beneath the search box. Then, click the dropdown menu to the right of ***Region***. This option will allow you to filter results by almost any region in the world.

7. **Choose how you want to receive the results.** Click the *More options* link beneath the search box. Then, click the dropdown menu to the right of ***Deliver to***. You can choose between your email address or an RSS feed. (You'll probably just want to choose "email address.")

8. **Click "Create Alert."** After you have made all your choices and the results preview is to your satisfaction, click ***CREATE ALERT***. You will now receive alerts to either your e-mail address or your RSS feed

CHAPTER 3

What to do if You Already Have Been Scammed

- If you used your bank for the scam transaction, contact them immediately to see if they can stop or reverse your transaction.
- Call your local police to report the crime.
- File a report with the Federal Trade Commission, either online or call 877-382-4357. (You may also want to call your state's attorney general and consumer protection offices.)
- Report the scam to the FBI IC3 at www.ic3.gov.*
- If you sent the money through Western Union, call their fraud hotline at 800-448-1492.
- If you wired the funds through MoneyGram, call 800-926-9400 to alert them to the fraud.

CHAPTER 4

What to Do if Your Personal Data Has Been Breached

Have you checked yet to verify if your social security number was one of the 2.9 billion in the recent breach? Here are some of the reputable sites you can use to check your data's security:

NPDBreach.com*

NPD.pentester.com*

haveibeenpwned.com* – This is a popular site for discovering how much of your personal data is on the "dark web." (If you were wondering, the term "pwned" was coined by gamers to mean 'owned' (the 'o' was replaced by a 'p' because the two letters are right next to each other on the keyboard). The question '***Have I been pwned?***' means you are asking if someone has taken control of your email address, or if someone has created a user profile with your email address.

If you find that your Social Security number or personal data has been breached by the NationalPublicData.com cyberattack, three separate class-action lawsuits* have already been filed in the U.S. District Court for the Southern District of Florida, and you can potentially join these lawsuits. They are as follows:

- *Lowanda Wilcox v. Jerico Pictures Inc., Case No. 0:24-cv-61418-AHS;*
- *Barry Cotton et al., v. Jerico Pictures Inc., Case No. 0:24-cv-61396-MD, and*
- *James Thomas Jones v. Jerico Pictures Inc., Case No. 0:24-cv-61412-XXXX*

These plaintiffs are represented by the following law firms:

- *Kopelowitz Ostrow Ferguson Weiselberg Gilbert and Markovits, Stock & Demarco LLC*
- *Morgan & Morgan Complex Litigation Group, and*
- *Chimicles Schwartz Kriner & Donaldson-Smith LLP.*

CHAPTER 5

What the FTC Recommends You Do

If you already know your Social Security number has been breached at some point, the Federal Trade Commission recommends you take advantage of any offer for free credit monitoring, if the company responsible for exposing your personal information offers it. While we're on that topic, the company responsible for the breach may or may not be legally required to pay for your credit monitoring subscription. This depends on:

- **Jurisdiction:** Laws will vary by state or country.
- **Terms of Service:** The company's privacy policy should state the terms of service, and some offer identity theft protection as part of their policies.
- **Negligence:** If the company was negligent in protecting your data, they may be held liable for damages, including identity theft protection services fees.
- **Class-Action Lawsuits:** You may be asked to join a class-action lawsuit against the company who exposed your data, and this could lead to compensation.

CHAPTER 6

How Sonata Bank Protects Your Data

These are the strategies and protocols Sonata Bank has deployed to protect our customers' data and funds from bad actors:

Multi-Factor Authentication (MFA)

- **What it is:** We require our customers to provide two or more verification factors in order to gain access to their accounts.

- **How it helps:** This adds an extra layer of security, making it harder for attackers to gain unauthorized access, even if they have our customer's password.

Encryption

- **What it is:** This is what converts data into a code that prevents any unauthorized access to our customers' accounts.

- **How it helps:** This system ensures that sensitive information (e.g., account numbers, personal details) is protected when stored or transmitted, making it unreadable to anyone without the decryption key.

Secure Email and Communication Channels

- **What it is:** We use secure email gateways and encrypted messaging platforms for our customer communications.

- **How it helps:** This prevents phishing attacks that rely on deceptive emails or fake websites by ensuring all official communication is secure and recognizable.

Regular Security Audits and Penetration Testing

- **What it is:** Sonata Bank conducts regular audits of our bank's systems to identify any vulnerabilities before any bad actors can.
- **How it helps:** These protocols enable us to proactively address security gaps before they can be exploited by cybercriminals.

Firewalls and Intrusion Detection Systems (IDS)

- **What it is:** We deploy network security measures to monitor and control incoming and outgoing network traffic.
- **How it helps:** This protects our customers against unauthorized access, malware, and other cyber threats by filtering traffic and detecting suspicious activity.

Proactive Customer Learning and Awareness Campaigns

- **What it is:** Awareness campaigns such as this eBook provide our valued customers with the information they need to recognize phishing scams, perform safe online practices, and know what to do if they suspect fraud.
- **How it helps:** This empowers our customers to feel good about protecting themselves because they will be able to recognize and avoid common scams.

Account Activity Alerts

- **What it is:** We send real-time alerts to our customers about any changes in their transactions or accounts.
- **How it helps:** This ensures our customers can quickly detect and report unauthorized activity, minimizing potential damage.

Tokenization

- **What it is:** This system replaces sensitive data with a unique identifier (token) that cannot be exploited if intercepted.
- **How it helps:** This protects customers' card information during transactions by ensuring that the actual card details are never transmitted or stored.

Anti-Malware and Anti-Phishing Software

- **What it is:** Sonata Bank utilizes specialized software to detect and block malware and phishing attempts.
- **How it helps:** This prevents malicious software from infiltrating banking systems and stops phishing emails from reaching customers' inboxes.

Behavioral Biometrics

- **What it is:** We analyze patterns in how our customers interact with their devices (e.g., typing speed, mouse movements).
- **How it helps:** We detect any anomalies in behavior that might indicate fraud or identity theft, which allows us to take action before a breach occurs.

Thanks for Reading About Cyber Threats

This eBook is designed to help you to better understand the dangers of emerging cybersecurity threats, the existing safety protocols you can exploit, and the protective measures you can take to identify and prevent potential threats so you can protect yourself from becoming the next victim of unwanted criminal activity. Sonata Bank appreciates your business, and we thank you for your time and attention.

**You will be linking to another website not owned or operated by Sonata Bank. Sonata Bank is not responsible for the availability or content of this website and does not represent either the linked website or you, should you enter into a transaction. The inclusion of any hyperlink does not imply any endorsement, investigation, verification or monitoring by Sonata Bank of any information in any hyperlinked site. We encourage you to review their privacy and security policies which may differ from Sonata Bank.*