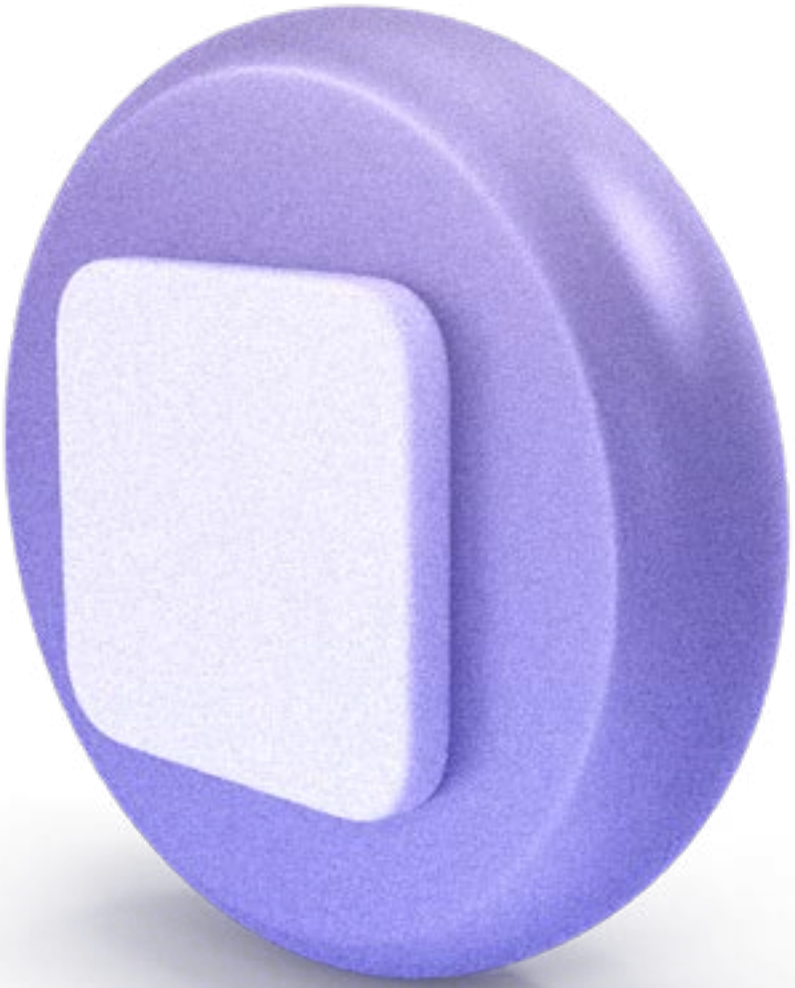
FS-ISAC

Stop the Scams: A Phishing Prevention Framework for Financial Services

A Publication of the FS-ISAC Fraud Strategy Working Group



November 2024

Executive Summary

Phishing is the most reported of all crimes[1] and financial services firms and their customers are frequent targets. The crime involves email, text messages, and telephone calls made under the guise of a trusted source – such as a bank or other financial institution – to obtain personal, financial data, and/or login credentials.

Victims of these scams can face severe financial damage and lose trust in the financial services ecosystem. Their financial services providers may be accountable for voluntary or legally mandated remediation of the consumer's financial loss.

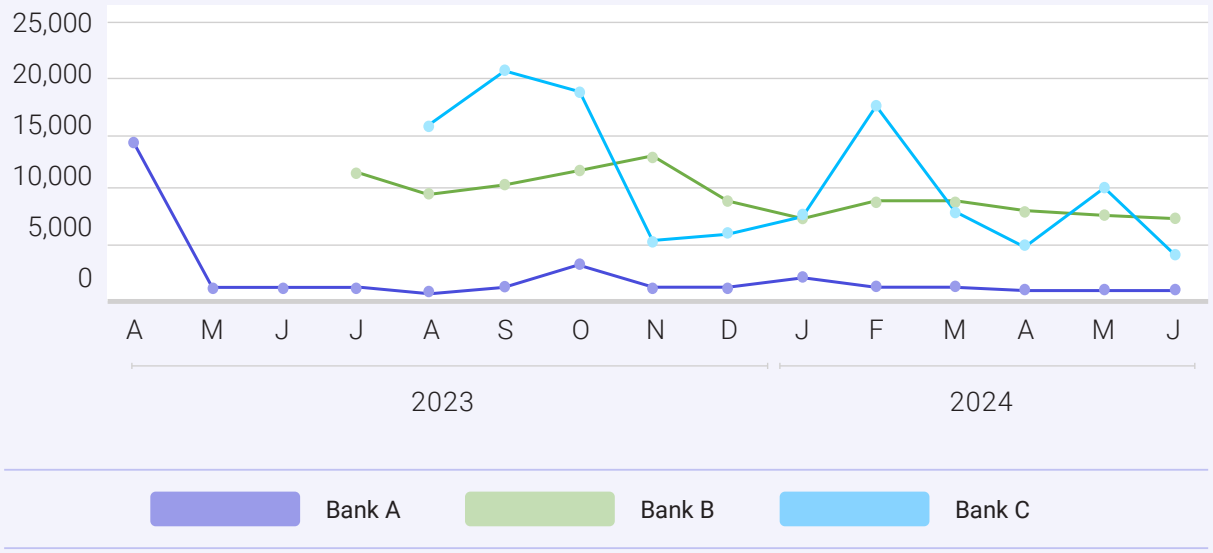
As with all threat prevention, there are no silver bullet solutions. Three FS-ISAC member firms, all large US banks, have implemented enhancements and controls that reduced reports of text abuse volume by half or more in a matter of months. Their approach is based on these key actions:

1. Obtain actionable intelligence from consumers and share it cross-functionally
2. Provide internal and external education
3. Catalog every telephone number used internally and by third parties
4. Leverage telecommunication providers' anti-phishing solutions

One bank saw a **90%** reduction in abuse box reports

These member firms shared their approach with the Fraud Strategy Working Group, who then collaborated to develop this Phishing Prevention Framework. The Framework applies to firms of all sizes and maturity levels.

Impact of Phishing Prevention Framework on Reported Scam Attempts



1 https://www.fbi.gov/news/press-releases/fbi-releases-2023-crime-in-the-nation-statistics

Best Practices to Make the Framework Work For You

Each of the following best practices is linked to the appropriate step of the Phishing Prevention Framework. Implementing these best practices will make each step of the process more effective.

- **Design a Fraud and Phishing Report Intake Process that gets actionable answers**

Financial institution fraud reports often focus on identity verification of the reporting consumer and gathering transaction-specific information to determine what action is required. Carefully planned questions and proper internal training can maximize this pivotal discussion to obtain critical pieces of intelligence, without adding a lot of extra time to the intake process.

- **Build an Abuse Box infrastructure that facilitates information sharing**

Providing consumers with the means to report attempted scams garners timely, firsthand knowledge of threats. Fraud teams benefit from that intel – but so do other internal teams and the financial sector as a whole. For that reason, design abuse box infrastructure and training programs that maximize the insights and make it easy to share the information. Aggregated shared signals could lead to preventative actions.

- **Use Consumer-Facing Education and Awareness to tell consumers what to expect from you**

Determine how the firm will communicate with consumers and let them know what to expect. That way, consumers will know that unexpected types of communication are potentially fraudulent. This is an ongoing aspect of fraud and scam prevention – not a step in the Framework. Consumer education and awareness are always key to stopping the scams.

- **Do Internal Telecommunications Research to identify every means of communication**

Gather the appropriate cross-functional internal teams to uncover every possible communication method used within the organization and by third parties on the firm's behalf. That process enables a full evaluation of communication vehicles, surfaces those that should cease, and indicates methods that require new or different controls, retention methods, resiliency plans, etc.

- **Engage with Telecommunications Providers to discover their phishing prevention capabilities**

Your telecommunications partners may have embedded and add-on capabilities to assist in phishing prevention. Some have access to data that can help you:

  - Identify threats
  - Gather the characteristics needed for tracing call sources
  - Determine additional rules or controls
  - Fulfill regulatory requirements, such as checking phone numbers against the Reassigned Numbers Database

These approaches can enhance anti-phishing strategies, help eliminate incorrect contact information, and prevent penalties.

It may be necessary to find and engage the right people internally and with providers in strategic discussions. Employees and third-party providers can have a big impact on customers' telecommunications with the firm and its solutions.

Note that internal teams – such as cybersecurity, fraud, business, product, infrastructure, communications, and legal – should understand the Framework and be engaged from the start. The Fraud Strategy Working Group recommends keeping those people in mind during the Framework's implementation. FS-ISAC members will find that their peers in the Fraud Strategy Working Group are resources, too, and can offer advice on the ongoing aspects of the Framework.

Putting the Phishing Prevention Framework Into Practice

The steps of the process are rank ordered – the most fundamental are at the beginning – so that it can be tailored to the needs of the institution. Nonetheless, implementing any step of this process will present an obstacle to threat actors.

The process is split into six sections, but because threats intersect, some steps may need to be conducted at the same time or in a different order.

	Framework Legend
1	Step 1
2	Step 2
3	Step 3
↻	Ongoing

Phishing Prevention Framework

	Fraud and Phishing Report Intake Process
	Objective: Ask questions that maximize fraud reports to make a full determination of how the threat actor initiated contact or gained access.
1	Evaluate your current frontline fraud and phishing reporting process.
1	Research any critical pieces of insight missing in the process to consistently determine the source of fraud and gain enough information to report for future prevention.
2	Work with internal teams to build a strategy to implement enhanced intake questions, which will require explaining the need and gaining their buy-in.
2	Develop a brief, yet effective, template of data collection questions for fraud and frontline staff to use for fraud reports. Questions should obtain: > Transaction details of any fraudulent activity > Phone numbers (including caller ID and recipient numbers) > The date and time of call, text, or email > Email addresses > The sender and recipient > Message or discussion details > Images of messages > Applicable phone history
2	Determine which internal teams (i.e. fraud, cybersecurity, compliance, internal and external training) should receive the individual reports.
3	Define procedures for real-time sharing with appropriate teams.
↻	Educate internal teams on the updated process.
↻	Evaluate the current frontline fraud and phishing reporting process.
↻	Research the process to determine if any critical pieces of insight are missing that would consistently identify the source of fraud and gain enough information to effectively report for future prevention.

	Abuse Box
	Objective: Set up an infrastructure that supports reporting, then aggregate the signals.
1	Evaluate the volume of fraud reports that resulted from phishing to provide a baseline for metrics.
1	Engage all impacted internal teams for a project review and to define the implementation strategy.
1	Implement internal abuse box email folders, access, and workflow.
1	Develop a process to report on activity details and trends. The process will likely be manual in the beginning but can progress to greater automation.
2	Review existing internal reporting processes to identify enhancements needed to build a repeatable, measurable process to triage phishing reports in a timely manner, including a feedback loop to reporting consumers.
2	Evaluate website enhancements needed to facilitate the abuse box creation.
2	Implement internal training on threats and reporting processes, and draft a FAQ to support consumer inquiries.
2	Execute a consumer education and awareness plan (see Consumer-Facing below).
3	Set a regular time to review progress with all impacted parties and be flexible to adjust the process as needed.
↻	Research any hurdles to sharing abuse box reports with industry partners (i.e. intelligence, telecommunications, and email gateway service providers) to maximize disruption of telecommunications attacks.
↻	Create and implement an abuse box intelligence sharing process (internal and external).

	Consumer-Facing Education and Awareness
	Objective: Set up an infrastructure that supports reporting, then aggregate the signals.
1	Draft messaging for consumers to define the type of communication they will receive from the institution going forward so they know which messages can be expected and trusted.
2	Evaluate key recommendations to consumers to maximize scam prevention: use multi-factor authentication (MFA), vary passwords, use a password manager, and take advantage of telecommunication provider tools such as reporting spam to 7726, blocking robocalls, or texting OFF to 4040 to block email-to-SMS (for Verizon customers).
3	Develop a list of critical pieces of information to request from consumers (see Fraud and Phishing Report Intake Process below).
↻	Establish consumer education on when, where, and how to report phishing attempts.
↻	Refine consumer education of phishing threats as needed due to evolving threats or processes.

Internal Telecommunications Research	
	Objective: Catalog your communication methods – both outgoing and incoming – with your consumers.
1	Evaluate all aspects of your own telecommunications space. This critical first step will take time, so start early. Document all current communication methods to consumers, including phone, email, text, SMS short code, email-to-SMS, website, etc.
1	Work across all business units to identify all the phone numbers and short codes used for consumer outreach, along with a process for any future forms of communication. Classify each phone number and short code as known bad or known good (numbers known to be used by the firm, including those used through third-party providers like call or fraud prevention services).
2	Execute consumer education and awareness plan (See Consumer-Facing, above).
2	Partner with internal teams to ingest and action any available activity reporting.
3	Determine if any current communication methods will need to be modified or eliminated for clear and consistent messaging to consumers of what is to be expected, especially when eliminating email-to-SMS.
3	Determine if it is possible to denote key phone numbers that are inbound-only on the DNO (Do Not Originate) registry.
↻	Update processes as necessary to remove any known email-to-SMS communications. Carriers may voluntarily sunset this function, so it's important to know if and where it is used and how to eliminate it.
↻	Develop an implementation plan for any necessary adjustments.
↻	Define a process for continuous message content filtering to better prevent the delivery of malicious text messages.

	External Telecommunication Provider Engagement: DMARC (email-to-SMS), Do Not Originate, Call Signing
	Objective: Identify your telecommunication providers' phishing prevention resources.
1	Meet with carriers to determine all fraud prevention and reporting options available to your organization as you investigate enhancements.
1	Evaluate options to define DMARC to eliminate email-to-SMS. Carriers may voluntarily sunset email-to-SMS.
1	After evaluating internal telecommunications, meet with carriers again to build a strategy to take advantage of advanced solutions and reporting options.
1	Determine what is most critical to track (spoofing frequency, impact, etc.).
1	Evaluate data sources (manual call tracking, vendors, partners, known good calls, internal teams/fraud, telephone infrastructure).
2	Investigate providers' processes to implement DNO on inbound-only phone numbers.
2	Work with telecommunications providers to evaluate available options to receive detailed call activity to aid in data analysis and threat reporting.
2	Determine if the provider can utilize honeypots to find illegal calls.
2	Track activity.
3	Examine options for call signing to align to STIR/SHAKEN [Secure Telephone Identity Revisited (STIR) and Signature-based Handling of Asserted Information Using Tokens (SHAKEN)], which enables unlawful call identification through call fingerprinting.
3	Develop a plan to implement identified solutions after internal processes and training are complete.
↻	Define a regular check-in with providers to discuss fraud trends, recommendations, and needs.
↻	Analyze the trends to get a baseline on your reported activity.
↻	Fill in data gaps.
↻	Analyze data to provide insight into threats, prevention efforts, enhancement opportunities, and the wins to celebrate.

Conclusion

There are many options to maximize phishing prevention, all of which can be enhanced by this framework. Though it may take some time and expense to implement some of the steps, the process ultimately increases efficiency (fewer reports to process), decreases fraud, and results in happier consumers. That impact will grow as more advanced measures are added.

That said, a singularly effective anti-phishing method is sharing information about malicious activity. One institution's fraud experiences become preventative information when actionable intelligence is shared with the sector. Sharing insights – such as known bad phone numbers and emails, trends, and tactics – undermines criminal attempts and makes all institutions stronger.

> Criminals have mastered intelligence sharing on targets, hurdles, and much more, as their frequent communication on the dark web proves. To optimize prevention, the financial services sector needs to communicate more than its adversaries do.

Sharing phishing abuse intelligence in the FS-ISAC community also creates data we can correlate. That brings to light larger patterns of threats related to known bad actors that impact multiple members. As a result, FS-ISAC can collaborate cross-sector to seek additional methods to stop threat actors and fill intelligence gaps, leading to further fraud and scam prevention.

The leaders of the Fraud Strategy Working Group chose to share this process to raise the security posture of the entire sector. Together we will have a significant impact on the business model of the threat actors targeting us and all whom we are trusted to serve.

To join FS-ISAC or, if already a member, the Fraud Strategy Working Group, please contact us.

