Security Awareness Scavenger Hunt Guide: Engaging Minds and Increasing Retention

Adrian Kwitkowsky

Table of Contents

1 Introduction: The Power of Interactive Security Awareness

Death by PowerPoint stinks, so most “standard” trainings fall flat. After all, with retention rates around 10%, traditional training methods leave a lot to be desired, with critical information unabsorbed and behaviors unchanged. Enter the security awareness scavenger hunt! It’s a low-cost (or no-cost) dynamic approach that transforms dry policies into an interactive, memorable experience. Engaging methods like this boast retention rates of up to 75%, a marked improvement from your mandatory annual compliance training. There’s a lot that goes into the psychology of security awareness, a topic I’m passionate about and in the process of writing a larger work on, however it should be common knowledge that it’s easier to get people to remember something if there’s more than just words involved. You must get them to feel like they’re part of it. Enter: games!

This guide will equip you with the knowledge and tools to create an online security awareness hunt that not only educates but hopefully captivates your workforce and leaves them waiting for the next round. Whether you're a seasoned security professional or new to awareness programs, I hope you'll find actionable insights to elevate your organization's security posture.

My goal is simple: to help you craft an experience that integrates security awareness seamlessly into your company culture. After all, in a world where people are complicated and threats are evolving, shouldn't our training methods adapt? Let’s have some fun.

Planning Your Hunt: Laying the Groundwork for Success

2.1 Defining Your Objectives

By far the longest part of this guide, here we lay the groundwork that will maximize ROI and impact on your organization’s risk and security posture. Like they say at Papa John’s: Better Ingredients, Better Pizza! Before diving into the details of your hunt, it's crucial to establish clear, measurable objectives that align with your organization's most pressing security needs. While it might be tempting to create a general awareness hunt, which is great for smaller or less mature organizations without support structures like we discuss next, the most impactful approach involves collaborating with key departments to identify specific, current challenges.

Partnering for Precision

To truly hit the mark with your objectives, consider partnering with the following teams:

Security Operations: They can provide insights into the most common security events they're dealing with, helping you focus on real-world scenarios your employees might encounter.

Insider Threat: This team can highlight behaviors employees are currently doing that could potentially lead to internal security breaches, allowing you to address these risks in your hunt.

Threat Intelligence: They can inform you about current external threats, ensuring your hunt prepares employees for the latest tactics used by the bad guys.

HR or Compliance: These departments can identify which policies are most frequently violated, helping you point to key internal resources through your hunt.

By tapping into the knowledge of these teams, you're essentially crafting your hunt with "better ingredients". This collaborative approach ensures that your security awareness efforts are not just educational, but directly relevant to the current threat landscape and your organization's specific challenges.

Crafting Targeted Objectives

Armed with insights from these key departments, you can now craft objectives that are both specific and impactful. Aim to identify 3-5 key security concepts to reinforce through your hunt. Too many, and retention starts to fall off. These might include:

1. Recognizing and reporting the latest phishing tactics identified by your Threat Intelligence team.
2. Properly handling sensitive data based on the most frequently violated policies reported by Compliance.
3. Avoiding behaviors that commonly trigger security events, as identified by Security Operations.
4. Understanding and mitigating DLP events highlighted by the Insider Threat team.

Remember, the goal is to create a hunt that not only educates but also directly addresses the most pressing security behaviors and challenges within your organization.

A Foundation for Ongoing Improvement

It's worth noting that this collaborative approach shouldn't be limited to your scavenger hunt. Ideally, your entire security awareness program should be informed by regular input from these teams. However, I felt it was worth reinforcing it here at the start of our journey. This ongoing dialogue with those key teams ensures that your awareness efforts remain relevant, timely, and aligned with your organization's evolving security needs.

By laying this strong foundation of cross-departmental collaboration and targeted objectives, you're setting the stage for a security awareness hunt that delivers maximum impact and ROI, which your boss or your boss' boss' boss will like. You're not just creating a fun activity; you're addressing real, current security challenges in an engaging and memorable way, and impacting your company's security culture more than just a slide deck would.

In the next sections, we'll explore how to translate these carefully crafted objectives into engaging questions and challenges. But remember, the success of your hunt is largely determined by the thought and collaboration you put into this initial planning stage. Take the time to get it right, and the rest of your hunt will fall into place much more effectively, and just 'make sense'.

2.2 Determining Scope and Duration

Finding the right balance for your hunt's scope and duration is crucial. You want to maintain engagement without overwhelming your participants. A good rule of thumb is to aim for a duration of one to two weeks. This gives busy employees enough time to participate without the hunt losing momentum.

When planning your timeline, consider your audience's typical workload and availability. You might also want to align your hunt with other security initiatives or events, such as Cybersecurity Awareness Month in October.

For larger organizations, consider a rolling launch across departments. This approach can help manage the load on your IT and security teams, ensuring they can provide adequate support throughout the hunt.

Optimal Duration

A duration of one to two weeks often works well. This gives busy employees enough time to participate without the hunt losing steam. However, consider your organization's unique rhythm:

- For smaller, agile teams or targeted hunts, a shorter, more intense hunt of 3-5 days might be more engaging.
- Larger corporations might benefit from a longer, multi-stage 3-4 week hunt with weekly themes or challenges.

Scope Considerations

When defining the scope, consider:

- Number of questions or challenges: Subjective! But, aim for 10-25 total, depending on complexity and the maturity of your security culture.
- Difficulty progression: Start easy and gradually increase difficulty to keep participants engaged.
- Time commitment: Each challenge should take no more than 10-15 minutes to complete.

Timing Strategy

Strategic timing can boost participation:

- Avoid major company events, end-of-quarter crunches, or holiday seasons.
- Consider aligning with Cybersecurity Awareness Month (October) for added relevance.
- For global organizations, be mindful of different regional holidays and work patterns.

Phased Rollout For larger organizations, a phased approach can be beneficial:

- Start with a pilot in one department to test and refine your hunt.
- Roll out to different departments or regions in stages to manage support load.
- Use learnings from each phase to improve subsequent rollouts.

2.3 Selecting Your Platform

The platform you choose for your hunt can significantly impact both the user experience and your ability to manage the event effectively. There are several good options to consider:

Microsoft Forms offers seamless integration with Office 365 and provides a familiar interface for many users. If your organization already uses the Microsoft ecosystem, this could be a natural choice. Google Forms is a free, user-friendly option that works well for organizations using Google Workspace. It's intuitive and easy to set up, even for those without technical expertise. SurveyMonkey offers more advanced features and detailed

analytics, which can be valuable for in-depth analysis of your hunt's results. However, it may require an additional budget.

There are other platforms out there as well, but you'll get the overall idea by reviewing these three. There are pros and cons to any decision, so let's itemize.

Microsoft Forms

Pros:

- Seamless integration with Office 365 suite
- Familiar interface for many users
- Built-in data protection features

Cons:

- Limited customization options
- Basic analytics capabilities

Best for: Organizations deeply integrated with Microsoft ecosystem.

Google Forms

Pros:

- Free and user-friendly
- Excellent for collaboration and real-time editing
- Easy integration with Google Sheets for data analysis

Cons:

- May not meet stringent corporate security requirements
- Limited question types compared to paid solutions

Best for: Small to medium organizations or those using Google Workspace.

SurveyMonkey

Pros:

- Robust features including advanced logic and piping

- Comprehensive analytics and reporting
- Wide range of question types and customization options

Cons:

- Paid plans can be costly for large-scale deployment
- Learning curve for advanced features

Best for: Organizations needing advanced features and detailed analytics.

Custom-Built Solution

For organizations with specific needs or stringent security requirements, a custom-built platform might be worth considering. While more resource-intensive, it offers maximum flexibility and control.

Whatever you choose, key selection criteria when choosing your platform, consider:

1. Ease of use for both creators and participants
2. Data security and compliance with your organization's policies
3. Integration capabilities with existing systems (e.g., Single Sign-On)
4. Analytical tools for assessing participation and performance
5. Mobile responsiveness for on-the-go participation
6. Scalability to accommodate your entire organization

2.4 Assembling Your Dream Team

Creating an effective scavenger hunt is a team effort. You'll want to assemble a diverse group of individuals with complementary skills. A typical dream team might include:

A security expert (that’s you!) to ensure the accuracy and relevance of your hunt's content. But, feel free to reach out to others who specialize in certain areas, as they can help craft questions that address real-world security scenarios your organization might face.

A communications specialist can be invaluable in crafting engaging messages and promoting participation across the organization. They can help ensure your hunt's language and tone resonate with your audience. Reach out to your organization’s comms department and give them the scoop.

IT support is crucial for handling the technical setup and troubleshooting any issues that arise during the hunt. They can ensure a smooth user experience from start to finish,

and/or make sure all the sites you are sending folks to are not blocked by any firewall rules or other tools.

Consider including an HR representative as well. They can provide insights into company culture and help identify potential incentives that might boost participation.

Remember, the success of your hunt relies heavily on cross-departmental collaboration. Foster open communication among your team members throughout the process, encouraging them to share ideas and concerns freely. With the right team in place, you're well on your way to creating a memorable and effective security awareness experience.

Organizations are vast and diverse, so there are many others you could potentially reach out to.

Project Manager

- Coordinates efforts across different team members
- Manages timeline and ensures deliverables are met
- Handles resource allocation and budget management

Tip: Even if not a formal role, designate someone to oversee the overall project Great for larger orgs since they can assist with some of the planning so you can focus on the details

Content Creator

- Develops engaging and varied challenge content
- Ensures consistency in tone and difficulty across the hunt
- Collaborates with the you or a SME to maintain accuracy
- Could add some visual appeal to ensure the hunt form/site isn’t boring

Tip: This could be a technical writer or someone from your training team. Alternatively, reach out to someone in Marketing, they often can provide a fresh perspective

Legal/Compliance Representative

- Ensures the hunt complies with relevant regulations and company policies
- Reviews content for potential sensitive information
- Advises on data handling and privacy considerations

Tip: Involving legal/compliance early can prevent last-minute roadblocks. Not that big of an issue for smaller orgs, but for larger companies… <sigh>

Executive Sponsor

- Provides high-level support and visibility for the initiative
- Helps secure necessary resources and buy-in
- Participates in kick-off or awards to boost engagement

Tip: Choose a sponsor who is passionate about security and can champion the cause.

Designing Your Hunt: Crafting the Perfect Challenge

3.1 Creating Engaging Questions

The heart of your scavenger hunt lies in its questions. Your goal is to craft challenges that not only test knowledge but also encourage exploration and practical application of security concepts. We're also teaching employees that information about staying secure is out there, ready to be found. Aim for a mix that guides participants through both internal and external resources.

Consider an internal policy hunt question: "According to our Data Classification Policy, what color code is assigned to 'Highly Confidential' information?" This type of question familiarizes employees with crucial internal documents they might otherwise overlook. To aid participants, you could add a hint directing them to the relevant section of your intranet. Brownie points for you if you found out that proper data classification is a common issue from one of the areas you reached out to.

External resource exploration is equally important. A question like "Visit the CISA website and find their most recent alert. What type of threat does it address?" encourages employees to engage with authoritative security sources beyond your organization. There's a decent list of websites in the appendix to help you get started, but don't be afraid to go and explore the wild world of the internet for more resources.

Don't forget to include practical application challenges. For instance, "Log into our security awareness training platform. What's the title of the most recent module added?" This not only reinforces the importance of ongoing training but also ensures employees know how to access these resources.

3.2 Incorporating Various Question Types

Diversity in question formats is key to maintaining interest and catering to different learning styles. Multiple choice questions are great for testing specific factual knowledge, while short answer questions encourage deeper engagement with the material. Remember,

though: having open ended text input questions will require you to spend more time reviewing responses since there will be misspellings or errors.

True/False questions can be quick and easy, but use them sparingly to avoid oversimplification of complex topics. For a more interactive approach, consider file upload questions. These can be particularly useful for tasks like taking screenshots of completed security settings, providing tangible proof of learning application. Again, this approach is more “high touch” and comes with administrative overhead, so use it where you see fit and if you have the bandwidth.

3.3 Balancing Difficulty

A well-designed hunt should challenge participants without frustrating them. Start with easier questions to build confidence and engage participants from the outset. As the hunt progresses, gradually increase the complexity of your challenges. Keep in mind organizations have a very diverse population of employees. In my case, I need to ensure that both the CEO and a bank teller can both complete the challenge.

Include a mix of quick-answer questions and more involved tasks. This variety keeps the hunt interesting and allows participants to pace themselves. For particularly challenging questions, consider offering hints. This can prevent participants from becoming stuck and discouraged, while still promoting problem-solving. We want the overall experience to be positive, we’re not trying to trick people, but rather generate a feeling of accomplishment that will cement the lessons learned during the challenge.

3.4 Developing a Scoring System

While not essential, a scoring system can add an element of friendly competition to your hunt. If you choose to implement one, consider assigning point values based on question difficulty. This rewards participants for tackling more challenging tasks.

Time bonuses for quick completion can add an extra layer of engagement, but be careful not to prioritize speed over thorough learning. If it aligns with your company culture, you might implement a leaderboard to foster some friendly competition. Don’t force this part, because culture fit is very important.

Remember, the primary goal of your hunt is learning, not competition. Ensure your scoring system motivates participation without discouraging those who might not be top performers. The ideal system will encourage all participants to complete the hunt, regardless of their position on a leaderboard.

As you design your hunt, keep in mind that each question is an opportunity to reinforce key security concepts in an engaging way. In the next sections, we'll explore implementation

strategies, launch best practices, and methods for measuring the success of your hunt. These elements, combined with your well-crafted questions, will create a truly engaging security awareness experience with.... <drum roll please>... retention!

Implementation: Bringing Your Hunt to Life

4.1 Technical Setup

With your questions crafted and platform selected, it's time to breathe life into your hunt. This is where your planning transforms into a tangible experience for your participants, and also inspire you as you see it start coming together.

Start by creating your hunt on the chosen platform, working with whatever collaborators you've selected. As you build, keep in mind the user experience. Organize your questions in a logical flow, grouping related topics where possible. This not only makes the hunt more coherent but also helps reinforce key concepts.

Don't forget to include clear instructions at the beginning of the hunt. Remember, while the concept might be clear to you, it may be entirely new to some participants. A well-crafted introduction can set the tone and ensure everyone starts on the right foot. Always keep the audience in mind.

Consider implementing branching logic if your platform allows it. This can create a more personalized experience, adapting the difficulty or focus areas based on participants' responses. It's a bit like creating a "choose your own adventure" for security awareness. Again, added complexity here might add administrative overhead at the end, so keep that in mind.

Once your hunt is built, testing becomes crucial. Don't skip this step - thorough testing can mean the difference between a smooth, engaging experience and a frustrating one that turns people off from future initiatives.

Conduct tests across various devices - desktop, mobile, and tablet. You want to ensure a consistent experience regardless of how participants access the hunt. Pay special attention to how any images render and how easy it is to input answers on different screen sizes.

Enlist your team members to take the hunt, or if you've chosen to fly solo reach out to some colleagues. Fresh eyes can catch errors or unclear instructions that you might have overlooked. For this reason, it's also important to have a diverse group of testers, not just

from one team. Encourage them to approach it as a participant would, and to provide honest feedback.

Finally, time the hunt. You want to ensure it's completable within a reasonable timeframe. Remember, while you want the hunt to be challenging, you don't want it to become a time sink that interferes with regular work duties. Plus, no one wants managers complaining about training initiatives more than they already do.

By paying attention to these details during implementation, you're setting the stage for a smooth and engaging hunt that participants will enjoy and learn from. In our next section, we'll look at how to prepare the supporting materials that will help guide your participants through this adventure in security awareness.

4.2 Prepare Supporting Materials

The success of your hunt doesn't just rely on great questions - it's also about providing the right support. Think of this as creating your treasure hunter's toolkit.

Start with a comprehensive instruction guide. While we touched on this in the section above, if you're creating a more complicated hunt, like something with multiple stages, it's important that things are clear. This should cover the basics like how to access the hunt and any rules or guidelines, but don't stop there. Include a clear deadline for completion and, crucially, who to contact if participants run into trouble. Remember, the goal is to challenge, not frustrate.

Next, develop a FAQ document if you feel it's needed. In fact, maybe a FAQ is enough and you don't need both comprehensive instructions AND a FAQ. See what fits your hunt and your company culture. Anticipate common queries: "What if I can't find an answer?" "Can I retake the hunt if I don't do well?" "How will the results be used?" Addressing these upfront can save you from your favorite activity: responding to endless emails that could have been prevented.

Finally, create a resource list... IF you feel like it. This could include links to company policies, relevant external security websites, and any tools or platforms referenced in the hunt. However, you could chose the more advanced route and let folks find the information all on their own. This is a subjective decision based on your organization's culture and maturity, so it's up to you. Ultimately, you're not just testing knowledge here - you're teaching people where to find important information when they need it. If your organization's level of maturity from a security awareness standpoint is pretty low or you're just starting out, a little bit of a point in the right direction for your participants won't hurt.

4.3 Plan Your Communication Strategy

Even the most brilliantly designed hunt won't be effective if no one knows about it. That whole “if you build it they will come” doesn’t work outside of the movies. Your communication strategy is key to driving participation and excitement.

Work closely with your Comms department if you have one, and start by crafting a compelling announcement email or intranet article. Again, your communications channels (like everything) will vary based on your org and culture. The announcement should highlight the importance of security awareness, explain the concept of the scavenger hunt, and clearly state any incentives or prizes. Remember, training has a bad rep so you’re going to try and sell this a bit.

If you’re feeling creative, or have a buddy in Marketing, consider creating eye-catching posters for office spaces, design engaging intranet banners, and prepare social media posts for internal platforms. The more touchpoints, the better.

Plan for regular updates throughout the hunt duration. These could include participation rates to spark some friendly competition, interesting facts discovered during the hunt, or gentle reminders of approaching deadlines. Vary the tone and content to keep things fresh and engaging. No one likes repetitive stuff like they’d normally find in those lovely annual compliance modules!

Launching Your Hunt: Execution and Engagement

5.1 Initial Announcement

Launch day is here! Start with a bang by sending out your kickoff announcement through your chosen channel. Use an attention-grabbing subject line, keep the content concise but informative, and include a direct link to start the hunt. Make it fun if company culture allows for it, but try not to be too cheesy. It’s easy to spot someone trying too hard and that might turn folks off. Make it as easy as possible for people to jump right in from the announcement with a direct link if you can.

If possible, leverage leadership endorsement (remember that executive sponsor I mentioned earlier?). Having a senior executive send or co-sign the announcement can significantly boost participation. Ultimately security awareness needs to be adopted at the top in order for culture to shift, so take this opportunity to make that happen. Also, ask department heads to encourage participation in team meetings as well. If you have a Security Champions or BISO group, leverage them as well.

Don't forget to clearly communicate any incentives. Detail the prizes or rewards and explain how winners will be determined. A little friendly competition can be a powerful motivator, but always keep your company's unique culture in mind. (Have I said that enough? Probably not.)

5.2 Maintaining Momentum

Launching the hunt is just the beginning. Keeping enthusiasm high throughout its duration is crucial for success. You might be surprised when a late joiner ends up winning the prize.

Send regular updates to keep the hunt top-of-mind if needed. If it's a short hunt, though, don't overcommunicate. We have enough emails to check already, and you don't want to get annoying. Share participation rates to encourage friendly competition, highlight interesting facts discovered during the hunt, or offer general hints for challenging questions. The key is to keep participants engaged without giving away the answers.

Use multiple communication channels. While email reminders are useful, don't neglect other avenues like intranet announcements, MS Teams/Slack, or digital signage in office spaces. The more visibility, the better, but again try not to annoy folks. No need to burn political capitol and discourage them from the next event.

Create buzz with teasers. Share anonymized, intriguing responses if you've got open text fields in your hunt and something interesting shows up, or post countdown reminders as the deadline approaches. A sense of urgency can be a powerful motivator, you know, like they put in phishing emails. It works <shrug>.

5.3 Providing Support

No matter how well you've designed your hunt, some participants will need support. Be prepared to assist them effectively and, take a deep breath, with kindness.

Designate a point of contact for issues. Ensure they're well-versed in both the hunt content and its technical aspects. But, let's be honest it will just likely be you. Establish a system for tracking and resolving queries to ensure no one falls through the cracks.

Monitor for signs of confusion or frustration. Be ready to clarify questions or fix technical glitches quickly. If many participants are struggling with certain sections, consider adjusting the difficulty or providing additional hints. Lessons learned here will help you next time.

Address any concerns about cheating or excessive collaboration clearly, however those don't happen often in the realm of "go look this stuff up" games. We're running the equivalent of an open-book test here. Have a plan in place to investigate any reports of

misconduct in the rare case it might happen, but approach these situations with empathy and a focus on education rather than punishment.

Remember, the goal is to create a positive learning experience. By providing robust support, you're not just helping participants complete the hunt - you're reinforcing the idea that security is a collaborative effort, where asking for help is encouraged and valued.

Post-Hunt Activities: Learning from the Experience

6.1 Analyzing Results

Phew! It’s over. However, the real work is just beginning. Diving into the data will reveal valuable insights about your organization's security awareness posture and the effectiveness of your hunt.

Start by examining participation rates. Did you achieve the engagement levels you hoped for? Look for patterns in completion rates across different departments or locations. This information can help you identify areas of the organization that might need additional attention or a different approach in future initiatives. You could leverage someone like a BISO to reach out to areas that didn’t have much participation and see how you could engage them next time.

Next, dig into the performance metrics. What was the average score? How long did it take most participants to complete the hunt? Was there a date/time that the hunt answers were submitted more than others? Pay special attention to the questions that were most frequently missed - these highlight gaps in your current security awareness training that you can address in the future across various areas in your awareness program.

If this isn't your first awareness initiative, compare the results to previous efforts. Has there been improvement? Are there persistent problem areas? This longitudinal view can help you track the evolution of your organization's security culture over time.

6.2 Recognizing Participants

Celebration is an often-overlooked part of the learning process, but it's crucial for reinforcing positive behaviors and maintaining engagement. If you've used a competitive model, now's the time to announce your winners. Consider multiple categories - highest score, fastest completion, most creative answers, if applicable, to recognize different types of achievement.

But don't stop at the top performers. Highlight interesting or creative responses from throughout the participant pool. These examples not only recognize individual contributions but also serve as additional learning opportunities for the entire organization. Use them to reinforce key security concepts in a memorable way.

Finally, make sure to thank all participants. Emphasize that by taking part in the hunt, everyone has contributed to strengthening the organization's security posture. A small token of appreciation for all who completed the hunt can go a long way in encouraging participation in future initiatives.

Consider working with Marketing to perhaps get a small badge or icon made for participants, or if you want to really kick things up a notch and run these hunts on a regular basis, you can leverage something like a martial arts belt system where multiple consecutive completions rank you up. Maybe something cool to put in an internal email signature? Work with your Security Champions program to come up with something. While it may seem silly, from a psychological perspective recognition like this goes a long way.

6.3 Gathering Feedback

You can’t improve what you don’t measure, and that goes for data about your hunt as well. Gathering feedback is a great step for refining your approach and ensuring future hunts are even more effective.

Start with a brief survey about the experience. Ask about the difficulty level, enjoyment factor, and perceived value of the hunt. Include some open-ended questions to capture detailed feedback that might not fit into predefined categories. Marketing might have some survey solutions already in place, but…. great news! Whatever platform you used to deliver the hunt can also be leveraged for a survey.

For more in-depth insights, consider conducting focus groups or having a Q&A lunch and learn people can join to provide feedback. These discussions can often reveal nuances that might be missed in a written survey. Bonus points: you can take this opportunity to go over each of the questions and expand people’s understanding of the various awareness areas you chose to focus on.

Don't limit feedback to a one-time event. Perhaps encourage ongoing input by setting up a channel for employees to submit ideas for future hunts. This not only provides you with a wealth of creative input but also keeps the conversation about security awareness alive long after the hunt has ended. Plus, then employees have a vested interest in participating in future events and spreading the word because they were able to contribute.

Continuous Improvement: Evolving Your Security Awareness Program

7.1 Refining Your Approach

Armed with data and feedback from your hunt, it's time to look to the future. Start by identifying the strengths and weaknesses of your current approach. What elements resonated most with participants? Which areas fell flat? What things were hard to manage from an administrative standpoint? Use these insights to refine your strategy for future hunts.

Consider how you can address the knowledge gaps revealed by the hunt. Perhaps certain topics need more emphasis in your regular training programs. Or maybe some concepts need to be presented in a different way to improve understanding and retention.

Don't be afraid to experiment with new formats or technologies in future hunts. Stay curious! The field of cybersecurity is constantly evolving, and your training methods should evolve with it. Stay abreast of new trends in e-learning and gamification that could enhance your next hunt. YouTube is typically a great resource for this in my experience.

7.2 Integrating with Broader Security Initiatives

While the scavenger hunt is a powerful tool, it's most effective when integrated into a comprehensive security awareness program. Look for ways to connect the themes and lessons from the hunt to other security initiatives within your organization.

For example, could you use the most-missed questions from the hunt as topics for future lunch-and-learn sessions? Or perhaps you could create a series of micro-learning modules that expand on the concepts introduced in the hunt. Consider providing data from the hunt to the teams that you collaborated with during it’s creation. Let Insider Threat know that people struggled on their question, or inform Compliance that some folks had a hard time finding a policy that was part of the hunt.

From an overall program standpoint, consider how you can maintain engagement between hunts. Regular security tips, newsletters, or even mini-challenges can help keep security awareness top of mind for employees throughout the year, and keep people in the loop for the next game.

Measuring Return on Investment (ROI)

8.1 Understanding the Investment

When it comes to security awareness scavenger hunts, we're not looking at hefty financial commitments. Most enterprises already have access to platforms like MS Forms through their Office 365 subscription, or can use free tools like Google Forms. Even if you opt for a paid tier of a service like SurveyMonkey, the cost is minimal compared to more resource-intensive options like on-site escape rooms. The primary investment here is time - your time in creating and managing the hunt, the time your collaborators invest, and your employees' time in participating.

8.2 Defining Success Metrics

Traditional ROI calculations don't quite fit the bill here. Instead, focus on metrics that indicate a shift in your organization's security culture:

- Participation rates in the hunt and other security initiatives
- Improvement in security knowledge (measured through pre and post-hunt assessments)
- Engagement levels with security-related communications
- Frequency of reporting potential security incidents

These metrics paint a picture of growing awareness and engagement, which is the true 'return' on your investment.

8.3 Measuring Long-term Impact

The true measure of your hunt's success is its impact on your organization's security posture over time. After all, that’s the whole point of an awareness program, no? The real gold lies in long-term behavioral changes. One fun idea is creating a group in your Security Information and Event Management (SIEM) tool consisting of hunt participants. (Call the SOC, they’ll help.) Over time, compare this group's security incident rates with those of non-participants. Are you seeing a decrease in security events associated with your scavenger hunt veterans? Congrats! You’ve impacted security culture. Now go do it again. This kind of data can be powerful evidence of your hunt's impact.

Regular assessments, perhaps in the form of annual security awareness surveys, can help you track changes in employee knowledge and attitudes over time. Compare these results to your baseline measurements to demonstrate the value of your awareness program to

stakeholders. If you have a regular cadence of security assessments, compare the results of hunt participants vs those who have never tried their luck.

Ultimately, culture will not change from just running these events. This is just a small part of your overall program that will help push the maturity needle forward. Growing security culture takes a while, and this is just another way to keep continuous pressure of the flywheel of maturity growth. Keep it up!

8.4 Presenting Results

When it's time to showcase your findings to stakeholders, focus on telling the story of cultural shift. Storytelling, after all, is a very underrated and powerful tool. Highlight the minimal financial investment required to implement these hunts. Showcase the enthusiastic participation rates and increased engagement levels. If you have data showing reduced security incidents among participants, that's your headline. Don’t forget to use the word “risk”. Management loves that stuff.

Remember the power of qualitative feedback - stories of employees feeling more confident in identifying phishing attempts or taking extra steps to secure their accounts can be just as compelling as hard data. Capture some of this when you’re taking notes during feedback sessions or lunch and learns.

8.5 Continuous Improvement

Remember, the goal here isn't to produce a single, impressive ROI figure. That doesn’t exist with this type of thing. We haven’t reduced the phishing hook rate from 9% to 2%. The point is to demonstrate a gradual, persistent shift towards a more security-conscious culture, and this is just one of the variety of tools we have at our disposal to do so. Use the insights you gather to continuously refine your hunts, ensuring that each one builds on the success of the last. In this way, you're not justifying a single initiative, but showcasing the ongoing value of an evolving, engaging approach to security awareness. Great for job security, I might add.

Advanced Hunts: OSINT & Teaching Social Media Hygiene

9.1 Level Up Your Game by Creating Fictional Online Personas

So, you've gotten bored of sending your fellow employees to various websites to find a line of text. Worry not! We can spice things up with OSINT! Open Source Intelligence Gathering (OSINT) is fancy cyber speak for digging stuff up on people, places, or things from publicly available sources online. This approach can be leveraged to start teaching employees how easy it is to be sloppy on social media or other sites with personal or company data.

One major limiting factor with this advanced technique is that many of these sites are often blocked by company policy, so if you were to explore using this technique, ensure you utilize websites, message boards, or other places that can be accessed by all participants. We don't want to encourage employees to use their personal home computers for this, especially in a larger enterprise. It will likely be frowned upon.

While much more complicated than what we've discussed so far, this can be super fun and also a great teaching moment. The cornerstone of this advanced approach is the creation of fictional online personas, often playfully referred to as "sock puppet" or "burner" accounts. Craft digital lives for these characters across multiple platforms, mirroring the online presence of typical employees. Spread information across various social media sites with different privacy settings to create a realistic digital footprint.

9.2 Designing OSINT Challenges

With your digital characters in place, it's time to send your participants on a cyber sleuthing adventure. Challenge them to uncover details about these fictional lives, much like a real-world OSINT practitioner might. Here are some scenario examples:

1. The Oversharing Pet Owner: Jane Doe constantly posts about her dog, Fluffy, on Facebook. Participants must find how this could be used in password guessing or security questions.
2. The Routine-Driven Executive: John Smith checks in at the same coffee shop every morning on Instagram. Explore the physical security implications of predictable routines.
3. The Careless Desk Photo: Sarah Johnson posts a picture of her desk on LinkedIn, with a post-it note containing passwords visible in the background.

4. The Company Structure Revealer: Participants must uncover connections between personas on LinkedIn, potentially revealing a company's org chart.
5. The Disgruntled Employee: Find a Twitter thread where a persona complains about IT security measures at work, discussing the risks of venting about workplace issues publicly.

9.3 Leveraging Teaching Moments

As participants piece together the digital breadcrumbs, guide discussions on the security implications of each discovery. Explore how seemingly innocuous information can be weaponized by bad actors. Discuss not just the immediate security risks, but also:

- How this information could be combined with other data points for more sophisticated attacks
- The potential impact on both personal and organizational security
- Strategies for sharing information online more safely
- The importance of being aware of one's entire digital footprint, not just individual posts

9.4 Ethical Considerations and Guidelines

This advanced approach requires careful handling. Clearly communicate the fictional nature of the exercise to participants. Provide guidelines on ethical information gathering and emphasize that these techniques should never be used on real individuals without consent. Develop a clear code of conduct for the exercise, outlining what is and isn't acceptable. This not only protects your participants but also models responsible OSINT practices.

9.5 Applying Lessons to Personal Online Presence

If you chose to pursue this route, encourage participants to apply these newfound OSINT skills to their own online presence. Guide them through the process of reviewing their social media accounts, adjusting privacy settings, and being more mindful of what they share online. Help them understand how their digital footprint could affect not just their personal privacy, but the organization's security as well.

Note: While this guide provides a brief overview of incorporating OSINT elements into your security awareness hunt, the depth and complexity of OSINT-based training warrant a much more comprehensive exploration. I'm considering developing a separate, in-depth guide focused solely on advanced OSINT-based security awareness training. This guide would delve into more sophisticated OSINT techniques, elaborate scenario and account creation, ethical considerations, and strategies for translating OSINT findings into actionable security improvements. If this is something you're interested in, please reach out for further discussion on how we can create a resource that really pushes the boundaries of interactive security awareness training.

Conclusion: Empowering Your Security Awareness Journey

As we conclude this guide, let's recap the key takeaways from our deep dive into security awareness scavenger hunts:

1. Engagement is key: By transforming security training into an interactive, gamified experience, you can significantly boost participation and knowledge retention.
2. Customization matters: Tailor your hunt to your organization's specific needs, culture, and industry for maximum impact.
3. Planning is crucial: From setting clear objectives, having great collaborators, to preparing supporting materials, thorough planning sets the foundation for success.
4. Communication drives participation: A well-executed communication strategy can make the difference between a lackluster event and a company-wide phenomenon.
5. Continuous improvement is vital: Use the data and feedback from each hunt to refine and enhance future initiatives or other parts of your awareness program.
6. ROI demonstrates value: Measuring and communicating the return on investment or culture impact to management helps secure ongoing support for your awareness programs.
7. Advanced techniques can elevate impact: Consider incorporating OSINT elements to provide powerful, hands-on lessons about online privacy and security. Could be fun!

Remember, the journey to a security-aware organization is ongoing, culture change takes a LONG time, and each scavenger hunt is a step forward. You've now got the tools and knowledge to create an engaging, effective security awareness experience. Don't be afraid to start small – even a simple hunt can yield significant benefits. Also, don’t be afraid to go big. Have fun with this, and so will your employees.

The most important step is the first one. Take the plunge, create your first hunt, and watch as your colleagues transform into active participants in your organization's security culture.

Have any questions or need further guidance? Feel free to reach out to me, Adrian Kwitkowsky, on LinkedIn. I'm always happy to connect with fellow security awareness enthusiasts, or anyone really, and help you on your journey to creating a more secure, aware workforce. You can also leverage the Security Awareness Advisor on the ChatGPT

store which I've created and trained up with this guide in the event you would like to be walked through, or want to workshop some ideas.

Here's to your success in making security awareness an adventure rather than a chore. Happy hunting!

Appendix: Sites to use for online scavenger hunting!

Internal Sites!

I put an exclamation mark in that title because I wanted to catch your attention. Never forget, internal policies and procedures are typically acknowledged in annual compliance training, but rarely ever read. Use this opportunity to point to internal resources on your company's intranet! Speak with HR, Compliance, and the SOC to see which areas people might need a refresher in and have them dig up the answers themselves.

External Sites

Here's a comprehensive list of websites that you can use as targets for scavenger hunts. There are likely many more, but this is a good start! Go get inspired.

1. National Institute of Standards and Technology (NIST) https://www.nist.gov/cyberframework
2. Cybersecurity and Infrastructure Security Agency (CISA) https://www.cisa.gov/
3. National Cyber Security Alliance (NCSA) https://staysafeonline.org/
4. SANS Security Awareness https://www.sans.org/security-awareness-training/
5. Federal Trade Commission (FTC) - Consumer Information https://www.consumer.ftc.gov/topics/online-security
6. US-CERT (United States Computer Emergency Readiness Team) https://www.us-cert.gov/
7. Internet Crime Complaint Center (IC3) https://www.ic3.gov/
8. National Cyber Awareness System https://www.us-cert.gov/ncas

9. Open Web Application Security Project (OWASP) https://owasp.org/
10. Center for Internet Security (CIS) https://www.cisecurity.org/
11. Information Systems Security Association (ISSA) https://www.issa.org/
12. ISACA (formerly Information Systems Audit and Control Association) https://www.isaca.org/
13. National Cyber Security Centre (NCSC) - UK https://www.ncsc.gov.uk/
14. Australian Cyber Security Centre (ACSC) https://www.cyber.gov.au/
15. Canadian Centre for Cyber Security https://cyber.gc.ca/en/
16. European Union Agency for Cybersecurity (ENISA) https://www.enisa.europa.eu/
17. Anti-Phishing Working Group (APWG) https://apwg.org/
18. Krebs on Security https://krebsonsecurity.com/
19. Dark Reading https://www.darkreading.com/
20. The Hacker News https://thehackernews.com/
21. InfoSec Institute https://www.infosecinstitute.com/
22. Naked Security by Sophos https://nakedsecurity.sophos.com/
23. Security Week https://www.securityweek.com/
24. CSO Online https://www.csoonline.com/
25. Electronic Frontier Foundation (EFF) https://www.eff.org/
26. Privacy Rights Clearinghouse https://privacyrights.org/
27. Identity Theft Resource Center https://www.idtheftcenter.org/
28. Have I Been Pwned https://haveibeenpwned.com/
29. Cybersecurity & Infrastructure Security Agency - Stop.Think.Connect. https://www.cisa.gov/stopthinkconnect
30. National Cyber Security Alliance - Lock Down Your Login https://lockdownyourlogin.org/

Industry-Specific Sites

Here are some examples of industry-specific site awareness resources. There are many more out there, so this is just for inspiration.

Note: links may be changed by site owners, this document may not update.

Financial Services:

1. American Bankers Association (ABA) - Financial Education https://www.aba.com/advocacy/community-programs/consumer-resources/protect-your-money
2. Financial Services Information Sharing and Analysis Center (FS-ISAC) https://www.fsisac.com/
3. Federal Financial Institutions Examination Council (FFIEC) - Cybersecurity Awareness https://www.ffiec.gov/cybersecurity.htm
4. National Credit Union Administration (NCUA) - Cybersecurity Resources https://www.ncua.gov/regulation-supervision/regulatory-compliance-resources/cybersecurity-resources

Healthcare:

5. Health Information Trust Alliance (HITRUST) https://hitrustalliance.net/
6. Healthcare Information and Management Systems Society (HIMSS) - Cybersecurity https://www.himss.org/resources-cybersecurity-privacy-and-security
7. Health Sector Cybersecurity Coordination Center (HC3) https://www.hhs.gov/about/agencies/asa/ocio/hc3/index.html
8. National Health Information Sharing and Analysis Center (NH-ISAC) https://nhisac.org/

Manufacturing:

9. Manufacturing Extension Partnership (MEP) - Cybersecurity https://www.nist.gov/mep/cybersecurity-resources-manufacturers
10. Manufacturing Leadership Council - Cybersecurity https://www.manufacturingleadershipcouncil.com/category/cybersecurity/

11. ICS-CERT (Industrial Control Systems Cyber Emergency Response Team) https://us-cert.cisa.gov/ics

Energy:

12. Electricity Information Sharing and Analysis Center (E-ISAC) https://www.eisac.com/

13. Oil and Natural Gas Information Sharing and Analysis Center (ONG-ISAC) https://ongisac.org/

14. Department of Energy - Cybersecurity https://www.energy.gov/ceser/cybersecurity

Retail:

15. Retail & Hospitality Information Sharing and Analysis Center (RH-ISAC) https://rhisac.org/

16. National Retail Federation (NRF) - Cybersecurity https://nrf.com/resources/retail-library/cybersecurity

Education:

17. Research and Education Networks Information Sharing and Analysis Center (REN-ISAC) https://www.ren-isac.net/

18. Consortium of School Networking (CoSN) - Cybersecurity https://www.cosn.org/edtech-topics/cybersecurity/

Government:

19. Multi-State Information Sharing and Analysis Center (MS-ISAC) https://www.cisecurity.org/ms-isac/

20. Government Technology - Cybersecurity https://www.govtech.com/security

Transportation:

21. Aviation Information Sharing and Analysis Center (A-ISAC) https://www.a-isac.com/

22. Maritime Transportation System Information Sharing and Analysis Center (MTS-ISAC) https://www.mtsisac.org/

23. Surface Transportation Information Sharing and Analysis Center (ST-ISAC) https://www.surfacetransportationisac.org/

Telecommunications:

24. Communications Information Sharing and Analysis Center (Comm-ISAC) https://www.nationalisacs.org/comm-isac

25. CTIA Cybersecurity Working Group https://www.ctia.org/about-ctia/working-groups#cybersecurity-working-group