Security+

ON THE LOOKOUT

Organizational security auditing framework for teams, developed by Security Positive

Why Security Auditing?

Nine out of ten businesses get hacked every year. In 2016, there were 4,000 attacks on business every day, a 300% increase from 2015. Business size doesn't seem to matter; 60% of small and medium-sized businesses were hit in 2014, often because they're easier to break into. The damage can be greater, too; 60% of small business hacked go out of business within six months.

Hiring IT security talent is expensive, and even the best can't keep up with the millions of lines of malicious code developed daily. Making matters worse, phishing and other socially-engineered attacks that capitalize on human errors are on the rise, and have the ability to not only affect your team and your company, but your business partners and clients.

Whether you've only read about these hacks or experienced them yourself, you may be wondering how to protect yourself and your team from data losses, damages to your reputation, or interruptions to your work. You may have you even tried to use security tools and practices, and, more than likely, have just gotten frustrated and given up.

What You'll Find Here

Here at Security Positive, we've developed a three-part, security self-auditing framework to support you. Our method helps you discover how to maximize your security, understand how your team's behavior may expose you to risks, and match your security priorities with strategies for adopting solutions for your entire organization.

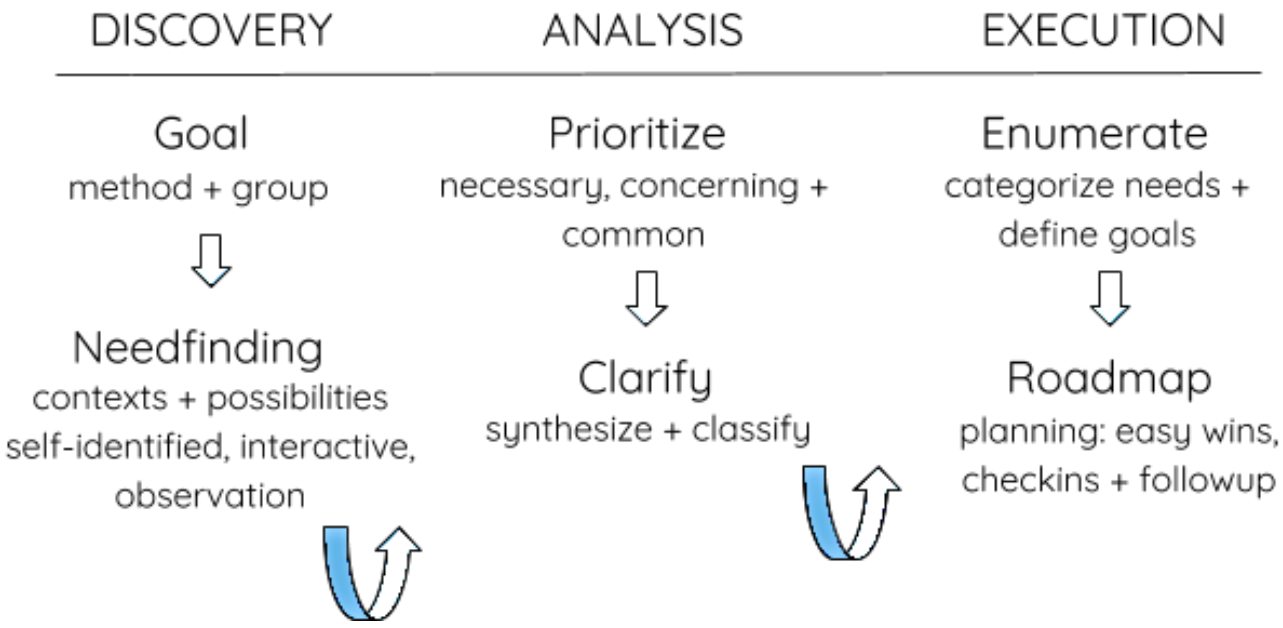
Our process is participatory for two reasons: we believe that human behaviors are the biggest risk to a team's security, and if you don't know what they are, you can't change them. Moreover, we find that asking for input and creating a solution in response supports adoption of new technology behaviors. In the first phase, Discovery, we cover what to consider for developing your participatory process -

60% of small business that are hacked go out of business within six months.

including your overall goal, the composition of the people involved, and how to map your resources - and offer templates, activities, and exercises to support you. Once you've gathered information on your needs, Security Positive offers methods to prioritize them according to the risk they pose and the ease of adoption. In the Analysis phase, you will review your most-often used tools and your sensitive information against common attack methods. This will clarify your strategy.

Finally, we provide roadmap exercises for implementing your strategy. In Execution, we break down your overarching goal into small and large goals to build momentum, and offer guideposts for creating a clear path to meeting them. The entire process looks something like this:

The Security Positive team developed and tested this auditing framework over the last several years, drawing expertise from the fields of national security, human computer interaction, psychology, human behavior, participatory methods, and trauma. In 2017, we created these exercises and activities to hand over the reigns to teams who wish to secure themselves. We can support you through our webinars and consulting services, and are happy to field feedback and questions. Email us at info@securitypositive.com.



Getting Started

Follow the below steps of the framework. Your may prefer to go through each step sequentially or repeat activities or entire sections in your process.

Discovery

In the first phase of this organizational security auditing process, you will gather data from your team through participatory methods. While participatory methods are called lots of things depending on how the data gathered is being used, the intent is the same: to elicit data from a group that enables you to build, design, or create something that will actually work for that group.

Security Positive subscribes to the notion that while people create security issues, they can also be a team's greatest resource for solving them. By working closely with team members to understand their needs, habits, and motivations, you can build a security process that will be responsive. That responsiveness - demonstrating that you've listened to your teammates and care about what they need and want - results in much higher rates of adoption of the security tools, practices, and policies you set. Participatory, responsive discovery sets you up for an efficient security intervention.

Setting a goal, determining a method

Your first and most important participatory action is to ask yourselves, each other, the whole team or a small group: Why are we doing this? What do we need? How do we know we're successful? What is our intended impact or goal, and how will we know we've reached it?*

If you're like most of us, you may think, "I'd like to make sure my team doesn't get hacked" or "we want to be more secure." Those are absolutely attainable goals with this framework. In the absence of clear indicators of success that are particular to your team and its context, the security process will be ongoing. Other teams may prefer to make a time-bound effort now, maybe another in a few months, and another next year. In this case, you'll want to determine how you know you've reached those goals. Is it when you've gotten secure communications locked down? Or when you feel confident your data is securely stored? Or maybe it's just having the analysis and a plan?

The specifics of your goal may become more clear as you begin your research. For more information on research goals and methods, check out the Internet Freedom Needfinding Framework, a resource created by our friends at SecondMuse.

Participatory Methods

> Coordinated set of activities and exercises that engage targeted groups of people to elicit data about needs, preferences, desires.

> Data are used to build, design, or create a tool, process, or technique for the group to adopt. Also called needfinding, human-centered design, ethnographic research, or contextual inquiry.

> Benefits:

- people are heard, not just listened to.
- they play active, influential part in decisions that affect their lives.
- diversity of methods inclusive of all kinds of learning + engagement styles.
- reverses learning: expertise is meaningless without local, contextual experience + knowledge.
- proven to better support longer lasting social change

Resources: Institute of Development Studies, IDEO, The Luma Institute, SecondMuse

Defining your working group

Over the years, we've tried lots of parameters for creating these groups, like changing the percent of staff involved, level of technical skill, and balance among genders, racial groups, ages, and other demographic factors. We've found that those parameters alone don't necessarily make for a cohesive working group. People need to feel heard and responded to. Thus, we've found having the following lead to higher adoption rates, namely:

- Individuals who act as champions of security, of a security process, of securing yourselves, or other goals you have identified along with increasing your security. Some may self-select, others you may select.
- Team members who you can easily identify as gatekeepers, role models, leaders, or cruise directors on their teams; leadership doesn't have to be defined by title.
- Some with technical skill, acumen and interest, and some who don't. You may include members who love gadgets or who are routinely asked for technical support by other teammates, and those who regularly need support or prefer to call rather than email, for example.
- A mix of people from project areas inside a team, or teammates across a company.
- We highly recommend connecting people who already work together on projects or teams. We encourage these working partnerships because they take advantage of an existing trust and will help one another reinforce new habits and behaviors.

Working group size has to be manageable for the team conducting the audit; if that's you alone, or just a few of you, keep the group size small. More data isn't necessarily better, and larger groups can be unwieldy in terms of logistics, and can also make the candor you need from your team a challenge. Alternately, more representation can yield more adoptable outcomes; if a small group doesn't produce

Who to include in your process?

We recommend creating a group of team members who represent a spectrum of knowledge, demographics, and project areas.

We also see great results when connecting people who already work together, especially if they like each other. They share a common language, they're used to each other's working styles already, and in many cases, they trust one another. Maximize the effectiveness of your process by building off of that trust relationship; you may even incentivize or create competition, as is appropriate to your work culture.

We liken these relationships to the accountability buddy systems common to exercise programs.

Outside the company? Most people work with people outside the company regularly, whether they're clients, partners, investors or funders, board members, or experts. It is really useful to include these folks, often more than worth the efforts required to accommodate logistics. Our primary recommendation if you choose to work with someone outside your team or company is that you pay close attention to circumstances, location and context and add any differences or exceptions to your overall risk assessment.

much representation, we recommend a series of smaller groups.

Next, you'll figure out how to set up the discovery process, requiring thought around the activities and exercises you'll perform with your team to gather data, and the logistics of conducting and processing that work.

Security Needfinding

All participatory processes offer data gathering from several sources, primarily self-reported, interactive, and observational. Each of these has its limits: people withhold when self-reporting out of a fear or judgement; interactive may be too daunting for those who aren't comfortable with other people; and observation doesn't always reveal what a person is thinking, just what they are doing. You may also wish to make use of verbal and visual activities. Ideally, gathering data from a combination of these sources can provide a clearer picture.

We suggest creating a method that balances your logistics - the time and workload constraints of your team, its skills and abilities, and any cash resources needed - with your understood need for security. To that end, we often conduct three activities, one from each of the self-reported, interactive, and observational categories, and a mix of verbal and visual:

	Self-reported	Interactive	Observational
Verbal	Questionnaire	Interview or focus groups	1:1 Processing
Visual	Visual Exercises from SecondMuse	Magazine cover, ideal future activity	Think-Aloud Usability Testing

Suggested strategies

+ Team in one location: Working with your team in one place, you may maximize your time together by running visual and verbal exercises in groups, with additional, more detailed information gathered from specific team members at a later time. **This model works best when you also have observers and notetakers documenting the process.** You may choose to run visual exercises and report back in a group, focus groups discussing a series of key questions, and think-aloud usability testing (see below) that builds on the ideal tool visual exercise.

+ Some distributed team: With a distributed team, we suggest conducting an initial questionnaire with all staff asynchronously, and then a focus group interview in person. We then ask distributed team members to complete and send in a set of visual exercises, and have headquarters-based staff complete the exercises as a group, with observation. An observational activity may be a VOIP-based, verbalized usability test, in which we observe a team member "trying out" a prototype of a tool, for example, and explaining to us what she does as she walks through it. If you have only a few distributed members, you may wish to conduct much of this process at a regular team gathering or retreat, or tacked on to a conference all or most of the team is attending. We suggest starting this process asynchronously for all team members, so that all feel they're part of the process, and not just the HQ staff.

+ Completely distributed team: This may be easier to conduct in small groups or with individuals. In the former case, we recommend creating groups

of teammates who already work together - **they will help one another reinforce new behaviors and tool usage.** In this scenario, it may be most useful to run visual exercises asynchronously, conduct individual or small group interviews, and conduct 1:1 processing out of the materials, in which a team member verbally describes a tool, an image, or an ideal situation.

Understanding your contexts + possibilities mapping

Threat modeling is the term that the information and digital security communities use to describe risk assessment. A threat model for teams requires an understanding of key pieces of information: your team members and how you all use technology; your location and specifics about your context; what you're doing when you interface with certain technologies; and who would like to take advantage of this information and what their capabilities are.

To begin, we'll look at how your team interacts with technology in various contexts. First, we'll identify areas of digital use, in this case: internal and external communications; data collection, transfer, and storage; devices, like laptops, phones, fitbits, and printers; connecting and browsing; your personal identifying information, including your social media accounts; and your physical security.

Then, we then look at how each team member uses technology in various contexts. We suggest looking at how your team interacts with technology in their work and personal lives, and in their work travels. If other contexts are appropriate, i.e., home offices or foreign offices, feel free to add those into the matrix.

To get started, open a copy of our Threat Impact Diagram. Have each team member complete it to gather the first half of your threat model information. Research on your context and adversaries and their capabilities can be completed in the ANALYSIS section below.

Resources

Sample Exercises + Activities

- Our sample questionnaire, which attempts to balance exhaustive data gathering with what will actually be completed by staff.
- Short questionnaires that can be administered by email or over a Google form.
- An exhaustive sample interview, heavily borrowed from Internews' SAFETAG project, and Engine Room's TechScape Project
- An intercept interview, a quick, three-question interview for getting immediately at motivations and needs. Adapted from Second Muse's framework.
- Some SAFETAG exercises
- Second Muse's templates

Additional resources for developing process

If you want to look at how others teach this method, SecondMuse and SAFETAG/LevelUp give ideas about setting up your process. IDEO lays out four different time- and knowledge-based scenarios for your process. The UN University's 2003 guide for participatory methods is an excellent resource for thinking through logistics and mapping your overall strategy. The Luma Institute categorizes its activities as observing, analysis, and action, and builds from among those categories to develop an overall strategy.

Analysis

Next, sort through the data you've gathered to discern your priorities, taking into consideration the guideposts of what is easy, necessary, and vulnerable. This will help to chart a roadmap, which we'll discuss in the EXECUTION step, that's effective both in its adoption across the organization and in meeting your goals.

Knowing your priorities is key to understanding your specific threat model. To do that, we focus on what your sensitive information is and where it lives, considering the common kinds of attacks for organizations like yours, and then figure out what are the most frequently used tools and practices in your organization.

This is an area where security knowledge is useful, and we've included some trusted and regularly-updated resources to guide you through specific security settings and safer alternatives to apps and tools.

Prioritization

Determining priority is important to threat modeling. We offer two methods for looking at your team's priorities. One is to complete the next phase of our Threats Impact Diagram. The second is our Security Impact Canvas, which was developed for individuals to understand their security priorities. You may combine each individual canvas to draw a broader team security picture.

Priority is a matter of clarifying where your vulnerabilities exist. Broadly speaking, vulnerabilities lie in two places: what's most important to you and what's easiest for hackers to get to. As you'll see, these often overlap; those are good places to start. Begin by:

Addressing what's most necessary: You know best what's sensitive; it's the stuff that's most secret or intimate, or most damning to your reputation, your business continuity, your sales pipeline, and your key partnerships. It can be as simple as bank account and credit card information, as strategic as marketing strategy and product development, and as mundane as email conversations about competitors or friends.

A note on security guides

Security guides offer all kinds of advice for all kinds of reasons; without a clear idea of your priorities, and your threat model generally, it may not offer much that is relevant to you. What's worse, digging deep into guides can produce a crippling overwhelm. Arguably, your organization doesn't need to suffer through implementing LibreOffice and Linux, as the privacy benefit of tossing Microsoft out probably is not worth the political capital you would have to expend to get everyone to change. Get clear on what you need and don't let the gobs of well-meaning and unrelated advice derail you.

Determining what's most concerning: Common attacks are where some security research comes in handy. Don't worry if you're not a security expert, you can still search for attacks on teams similar yours, e.g.:

- Is ransomware shutting down laptops and servers?
- Are databases getting hacked?
- Company Facebook pages permanently hijacked?

Generate a list of 3-5 kinds of attacks that could potentially affect you, either because

they've happened to teams with similar work, cases, or profiles, OR because you have similar hardware, software, systems, processes, social channels, or technological understanding.

Three things to consider when making the list: your location, context, and attackers. Our method assumes you are a US-based company, and that your staff, technology, and clients are sourced from or based in the US, and takes into consideration US data and privacy laws, and US- licensed surveillance systems. Likewise, in your research, you may want to limit possible vulnerabilities to other US companies. If you have team members outside the US, conduct a separate analysis for each location, and include information on hardware and physical security.

Secondly, trying to understand attackers and circumvent their attacks may become overwhelming. In many cases, attribution and motivation is impossible or too expensive to discern; often young hackers practicing their skills can target you for little or no ideological reason. Thus, we suggest sticking to attacks that parallel your team, its work, and capabilities, and strengthening security around what's most sensitive to your organization.

Focusing on what you commonly and frequently use: A good strategy for overall adoption is to first work on changing habits or behaviors for the things you commonly and frequently use. It ensures that you'll get a lot of repeat usage quickly, which tones the necessary muscle for changing behaviors overall. Moreover, securing the things you commonly use clears out a bunch of vulnerability with just a few changes, e.g., if you're on email 80% of your day and your email is secure, you've got a lot of security taken care of. Look at the Security Impact Canvas for each member of your team, and make a list of the tools you all use daily and across groups.

Securely collecting + storing your process materials

Gathering sensitive data, or storing a lot of technical data in one place could become a security risk. When collecting and storing data, we suggest at least one person uptake a a handful of one-sided security tools, such as Virtru for email, Peerio, or Dashlane for its data sharing feature, to communicate, and share and store data. Similarly, saving data on Dropbox, Google Drive, or another cloud service is secure if two-factor authentication is enabled.

Activities to clarify your analysis

We've developed templates to help visualize your priorities. To identify what's commonly used, we recommend our Security Impact Canvas for individuals and the Threat Impact Diagram for the team. When you're ready to add in your sensitive information and research around attacks, check out the Threat Impact Diagram Matrix, the pages that builds on the Threat Impact Diagram. Prioritize the areas that need support into top priority, longer-term priority, and ongoing priority bands.

SecureSWOT, built off of the tried-and-true method for analyzing data, is another method for reviewing your data that can offer some clarity in the form of overlaps, trends, and needs.

Resources

Security guides + resources:

Martin Shelton's regularly updated Current Digital Security Resources

Three guides for all, despite their feminist bent:

- HackBlossom's DIY Feminist Security
- Feminist Frequency's Speak up and Stay Safe(r)
- Our 9 Ways to Dodge Trolls

Front Line Defenders' threat modeling workbook

EFF's Security Self Defense Starter Pack Playlist

Schneier on Security, Swift on Security, Krebs on Security

Execution

Now we'll take the data we've analyzed and draw your roadmap to better security. The Threat Impact Matrix, SecureSWOT, and other visualization exercises determined your top-level needs, which we'll use to set concrete goals. Then we'll define a timeline and plan for the resources needed. Finally, we'll put it all together in a roadmap that clearly marks steps needed, including reflection points, to achieve your security goals.

Mapping your needs

To build out a roadmap for securing your organization, start with connecting the priorities you've identified to appropriate tools, practices, and policies. From either the Threat Impact Matrix or the SWOT-style analysis, map what tools, practices, and policies need to be implemented on this corresponding template, the Priority Assessment Canvas.

For example, if you find that email is a priority, fill in your research on tools, practices and policies that support securing email. In this case, you may find that Gmail or another end-to-end encrypted option is a good start, and develop a policy around setting up Hushmail or ProtonMail accounts for sensitive information. Perhaps tools like Virtru and PGP are options, as they're compatible with your email application, and policies about when to use them, or what constitutes sensitive information is drafted. Finally, you determine that team-wide practices for strong email include setting long passwords and using two-factor authentication across all email applications and devices.

Using the Priority Assessment Canvas template, fill in the tools, practices, and policies you need to secure up to five priority items. You will likely find overlap in the tools and practices, which will cut down on the work of adoption. Also, don't worry if there are 10 more items on the priority list; you can do this in phases, and it gets easier as you go along. Start small so that 1) you actually start and 2) you gain some traction.

Once you identify what you want to secure, lay out the tools, practices, and policies to get you there, **give yourself a time-bound, specific, and attainable goal.** We stress that it be time-bound and specific so you can lay out a complete and clear roadmap, at least for the first few times until you get the hang of it. Do this legwork upfront, and we promise, getting everyone on board will be much easier.

Laying out the roadmap

Start with what's easy. Behavior science research shows that a series of small wins unlocks the ability for groups and movements to adopt big behavioral and cultural changes. It also helps things to feel less daunting and overwhelming.

That's also why we recommend making one critical change at a time. To continue the example from above, if you find that email is a top priority, take your list of tools, practices and policies, and map them out according to behavior change best practices, your timeline, and the resources you have available. Use the Roadmap Planning Worksheet and Template to start. Plug in your goal:

"We will use secure email and chat communications internally on Project X across the 20 members of the sales, PR and marketing teams by the end of the fiscal year."

Next, **test the tools with your group,** recording their experiences in one of several ways: observe them downloading and testing the tools, or ask them to complete tasks within the app; ask them focused questions, in a group or individually, looking for specific reactions, preferences, or needs met; have them complete the table in the Roadmap Planning Worksheet to compare tool features. More resources on testing are in the Resources section below.

Your testing data guides your decision-making, so we recommend checking back with the testing group to let them know what you favor and why. If you get pushback, or a strong desire to use another tool, we recommend you honor that, maybe even find a way to make that tool or both tools work. If you're between a few options, we suggest preparing both. Our research demonstrates that choice among a small set of options increases adoption.

Once you've selected a tool, review accounts, devices, and platforms that you'll use to access the tool. For secure chat tools to be effective, for example, the email accounts and devices with which your team accesses the tools must also be secure. Secure your accounts with long, strong passwords and two-factor authentication. Safeguard devices by adding a passcode and enabling full disk encryption.

Now you're ready to create the implementation plan. This guide will help you to parse all the data you've gathered into a phased plan. Our method focuses on making changes stick, creating small wins, building momentum, and reflecting on and responding to team needs. First, complete this worksheet, adding the tools, practices, or policies you will implement to secure your communications, and all foundational changes to see what you steps you need to take.

Next, plan your phases. Use data from your focus groups to determine which tools may be easiest to implement. For example, you've learned that PGP can be the most secure, but your test group finds it hard to adopt. On the worksheet, you see a number of account and device changes you can implement with Virtru and PGP. So, to build momentum AND lay the foundation for PGP, you start with Virtru as your first phase, and PGP as a second phase.

Then, separate the immediate from the long-term. Long passwords are strong because it takes so long for a machine to guess combination of 26 characters, for example. But many long passwords aren't easy to remember. While a password manager is a great solution, it's yet another new tool for your team to learn. We suggest starting with one long password for your email account, and saving the password manager for a later step. Similarly, turn on two factor authentication for your email, knowing that after its mastered on email it can be implemented on other crucial tools, like social media, CRMs, cloud storage, banking, team management.

TOOLS: Virtru, Signal + PGP
ACCOUNTS: passwords and two-factor authentication (2FA)
DEVICES: pass codes + full-disk encryption (FDE)

Start with small wins and build in reflection points. Start with the stuff that's easy *and* effective; we recommend a tool or practice that's constantly used that does not require

much to put into place. To continue our example, you determine that passcodes are your first small win. You put a passcode policy in place, give a brief training, and a week or two later you ask your team how it's going for them. Passcodes are extremely important - they're the first line of defense, particularly if a device is ever lost, stolen or left unattended; they are also used to encrypt devices. By typing in a code every time they access their device over the course of week, your team is pretty painlessly securing a lot of their data AND priming themselves for bigger changes to come.

After a few changes are implemented, check in with your team - we've offered a few template questions on the worksheet. With the reflection data you gather, you may modify your plans, completely change course, or even abandon the plan altogether. It's more important to demonstrate you're responding to your team's needs than to stick with the original plan. Reflection and responsiveness also aid adoption as they increase the speed of change, create trust in the process, and get folks to think about security in all aspects of their lives.

Follow-up and reinforcement activities

Key to lasting behavior changes are reinforcement activities. There are lots of ways to follow up, to engage with your team, and to reinforce without being overbearing or letting the thread drop. It will take some practice for you to determine what works best for you and your team. In the meantime, try our Homework Activities Template to start.

Timeline, logistics, and resources needed to complete work

For each goal, you'll create a timeline. In the beginning, we suggest giving yourself plenty of time to figure out your process, and for your team to ask questions and iron out issues. Depending on what you're trying to implement and how responsive, cohesive, and technically savvy your team is, six months may be an appropriate amount of time for implementation of a few new tools and corresponding practices. You'll also want to consider resources and logistics: when and where trainings and check-ins are held, how much time the team has to donate to the efforts, and what additional materials may be necessary.

Behavior Change Methods

In this process, we incorporate behavior change techniques like small wins to build momentum and follow-up and reinforcement activities. There are numerous techniques that you can also incorporate and a large body of literature to dive into. We find the Fogg Behavior grid helpful for identifying kinds of behavior change, particularly GreenPath changes. We love The Power of Habit for identifying triggers and understanding motivations, and Thinking, Fast and Slow for understanding learning and working styles.

Resources

The Power of Habit and Thinking, Fast and Slow.

Homework + Follow-up Activities

Usability testing guides:

+ Interaction Design Foundation's Guide for Conducting Focus Groups

+ UT's Raven Veal on conducting UX research

+ Key differences in user testing groups and focus groups