bugcrowd

DATA SHEET

BUGCROWD SOLUTIONS

Social Engineering Awareness Solutions

Powered by **SocialProof Security**

Summary

Even simple Social Engineering attacks–including phishing, pretexting, and impersonation–can lead to massive breaches.

Although Social Engineering is among the most common attack vectors—and the #1 threat reported in ISACA's 2021 State of Cybersecurity Survey—many organizations are surprisingly unprepared for it, whether manifested by lack of organizational awareness, outdated or inconsistent identity verification protocols, shallow security practitioner skill sets, or all of the above.

Fortunately, a multi-dimensional approach comprising awareness training, protocol review, and pen testing can reduce that risk. Powered by SocialProof Security, Bugcrowd Social Engineering prevention services enable you to:

- Train all employees to notice and report attacks, and sharpen security practitioner skills
- Strengthen identity verification methods to stop account takeover
- Validate the effectiveness of training and protocol updates with a social engineering pen test

Offerings

Awareness Training: Live and Video

Train everyone in your organization to recognize and shut down social engineering attacks through real-world examples of hacking and mitigation (often fulfills compliance requirements for annual security awareness training)--live training and video library both available!

Protocol and Practitioner Workshops

Documenting and upgrading identity verification protocols is a critical step for social engineering defense. Similarly, upskilling your practitioner teams in the area has huge benefits. We offer workshop programs for both.

Penetration Testing

Want to assess the impact of training? The Social Engineering Pen Test measures your org's resistance to multi-channel attacks and/or account takeover. It includes a full report along with mitigation recommendations.

BUGCROWD SOLUTIONS

DATA SHEET

Social Engineering Awareness Training

RUNNING TIME	AUDIENCE LIMIT	WHO SHOULD ATTEND
60 MINS 45 mins of content 15 mins of Q&A	UNLIMITED	EVERYONE

Rachel Tobac, co-founder and CEO of SocialProof Security, has developed personalized, hands-on, and role-based events for Social Engineering Prevention training. These events–which can be described as talks, keynotes, or training sessions depending on your preference–are customized for each group, enhance awareness of social engineering in practice, and will arm attendees with the tools they need to mitigate human security risks.

These events are fast-paced, interactive, and gamified, and in many cases fulfill annual security awareness training compliance requirements for PCI-DSS, SOX, HIPAA, ISO/IEC 27001/27002, and GLBA.

ABOUT

Rachel Tobac

Rachel is a hacker and the CEO of SocialProof Security, where she helps people and companies keep their data safe by training and pentesting them on social engineering risks. Rachel was also 2nd place winner of DEFCON's wild spectator sport, the Social Engineering Capture the Flag contest, 3 years in a row. Rachel has shared her real-life social engineering stories with NPR, Last Week Tonight with John Oliver, The New York Times, Business Insider, CNN, NBC Nightly News with Lester Holt, Forbes, and many more. In her remaining spare time, Rachel is the Chair of the Board for the nonprofit Women in Security and Privacy (WISP), where she works to advance women to lead in those fields.

EXAMPLE TOPICS INCLUDE:

- Up-to-date and real life social engineering videos & script examples
- Live hacking demonstrations to showcase how to spot me in the act during an attack
- Why is social engineering relevant to my organization and role?
- How does social engineering impact my work?
- What are the recent social engineering attacks that have targeted roles like mine?
- What information do social engineers target (specific to my organization)?
- How do social engineers pick targets?
- How can I avoid becoming a target?
- Why does social engineering work on people?
- Example historic attacks: spear phishing and phone attacks, vendor compromise, business email compromise, etc.
- The tools social engineers use to attack
- How social engineers pick who they're pretending to be (specific to teams)
- How to spot a social engineer over email, phone, and in person
- What to do if you think you spot a social engineer
- Positive reporting culture and best practices your organization has in place
- Social engineering hands-on activities and participation

BUGCROWD SOLUTIONS

DATA SHEET

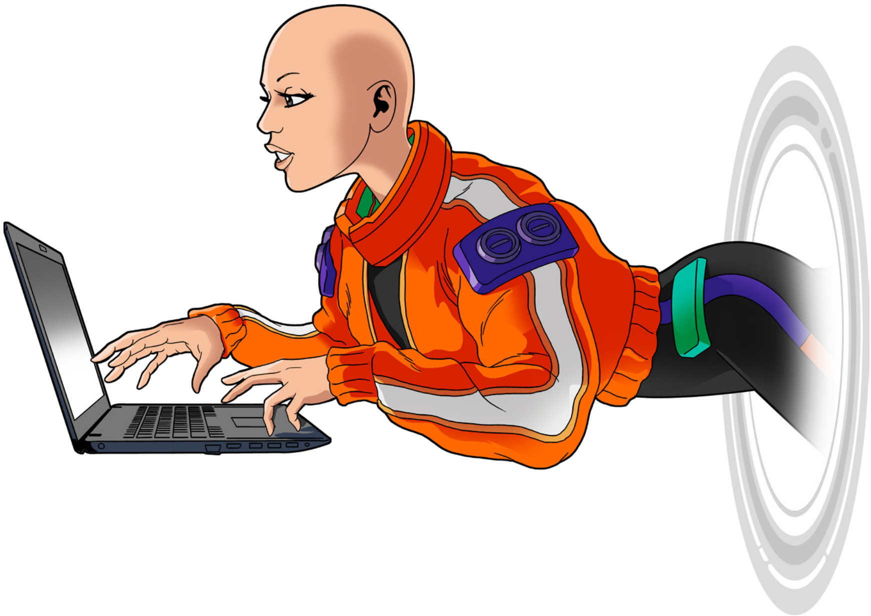
Social Engineering Protocol Update Workshop

RUNNING TIME	AUDIENCE LIMIT	WHO SHOULD ATTEND
90 MINS	UP TO 20	Customer Support, Finance, Sales, HR, Executives, External-Facing Employees

Many organizations are using outdated methods to verify the authenticity of requests and messages internally (making them susceptible to social engineering, fraud, business email compromise, ransomware, etc.) and externally (which allows social engineering criminals to perform account takeover of their client accounts, gain access to internal tools, and steal money and data).

This interactive workshop focuses on updating the identity verification methods used across the org to reduce the risk of account takeover, ransomware, financial loss, and more. In many cases, it will fulfill annual security awareness training compliance requirements for PCI-DSS, SOX, HIPAA, ISO/IEC 27001/27002, and GLBA.

By the end of the workshop, organizations will have a list of tailored identity verification protocol recommendations to mitigate social engineering risk at the client-facing level.



BUGCROWD SOLUTIONS

DATA SHEET

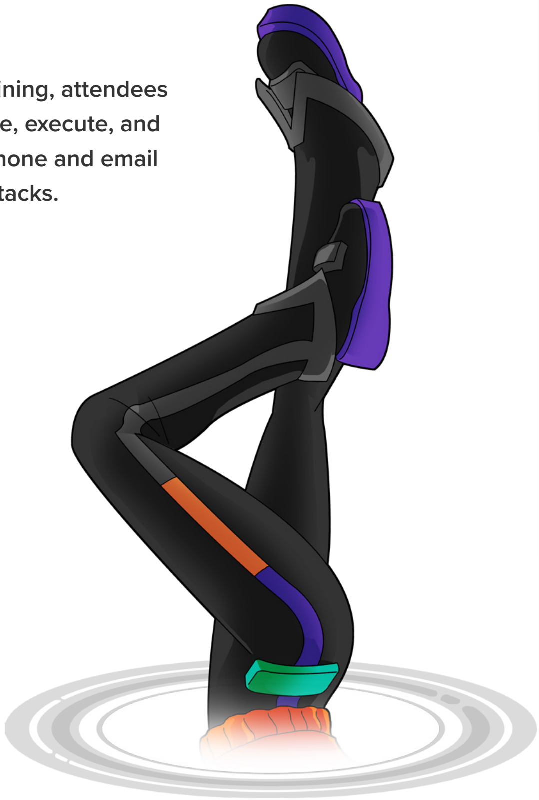
Social Engineering Practitioner Workshop

RUNNING TIME	AUDIENCE LIMIT	WHO SHOULD ATTEND
90 MINS	UP TO 20	Infosec, Investigators, Social Engineering Hobbyists, Red Teams, Blue Teams, Developers, IT Support, Helpdesk

The Social Engineering Practitioner Workshop is a live, virtual, hands-on engagement that focuses on OSINT, vishing, phishing, and social engineering training for Infosec, Red Teams, and practitioners to level up their social engineering skill sets.

This workshop is designed to enhance OSINT, social engineering, and phone/email attack abilities.

By the end of this training, attendees will be able to prepare, execute, and measure their own phone and email social engineering attacks.



WHAT'S COVERED:

- How social engineers use human behavior exploits to ensure targets comply
- Up-to-date OSINT and social engineering tactics from the field
- Real life social engineering videos and script examples
- The technical tools to use during OSINT and attack
- How to pick who to pretend to be (pretexting, impersonation, etc)
- How to select social engineering targets
- Your real-life target practice (controlled and safe hacking learning in real time)
- OSINT collection on your target
- Pretext selection for your target
- Picking individual targets within your target
- Script creation for attack
- Tabletop vishing and phishing walk-throughs
- How to authenticate and build trust through target challenges
- Vishing and phishing chaining (using information from one attack to the next)
- Hands-on social engineering activity; you'll get a real-life target and build an attack. Winners get prizes!

BUGCROWD SOLUTIONS

DATA SHEET

Musical & Spoken Security Awareness Training Video Library

RUNNING TIME	AUDIENCE LIMIT	WHO SHOULD ATTEND
~3 MINS EACH	Unlimited	Everyone

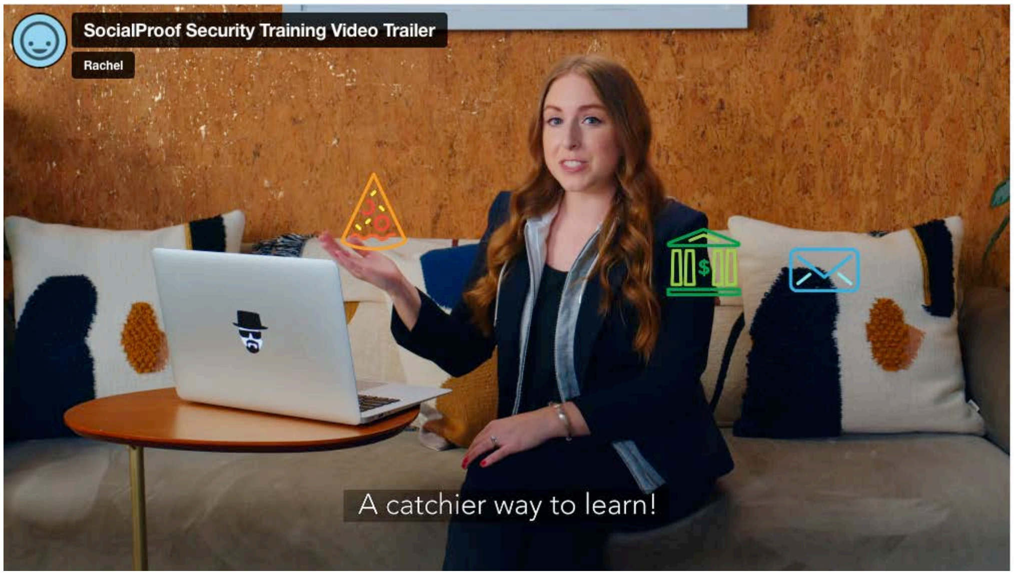
Rachel Tobac and the SocialProof Security team have developed a catchier way to learn with engaging musical and spoken security awareness training videos for your onboarding, monthly, or quarterly education -- with new videos released to the library often.

This training video library covers all the topics your team needs to know to catch and stop a cyber criminal in their tracks in quick and catchy 3-minute modules. Each song is a different genre, from alt rock to 80s bops, and every song has a companion spoken video with hacking demonstrations.

These SCORM compatible videos fit into your LMS (or we can host them on an LMS for you) with tailored logos, intros, knowledge-check quizzes, and takeaways customized for your organization.

EXAMPLE TOPICS INCLUDE:

- Malware & Ransomware
- Phishing
- Password Safety
- Social Media Safety
- Patching
- Reporting
- Multi-factor Authentication
- Social Engineering
- Up-to-date attack methods that cyber criminals use to trick teams, and much more



BUGCROWD SOLUTIONS

DATA SHEET

Social Engineering Penetration Testing

Social Engineering is among the most common attack vectors, but many organizations are unsure how they would fare in an actual social engineering attack scenario. Running a specialized pen test is the only way to assess how your org will respond to common real-world threats. This pen test takes place within a 1-week period, with precise timing determined mutually by both parties.

We recommend a Social Engineering Pen Test as a follow-up to our Social Engineering training and workshops in order to validate impact across your organization.

Complete

The Social Engineering Pen Test methodology can include phone, email, social media, chat/SMS, and account takeover to cover desired attack pathways.

Intensive

An industry leader in Social Engineering, SocialProof Security will employ all the classic, as well as the latest, techniques to accurately assess risk.

Validating

By stressing your defenses, the Social Engineering Pen Test validates that previous training and protocol updates are working.

Actionable

SocialProof Security will compile a full report and list of top mitigation recommendations to limit your social engineering risk.

Bugcrowd Penetration Test as a Service (PTaaS) Solutions

Web Application Pen Test

Test web applications, whether cloud-based or on-premises, of any complexity.

Network Pen Test

Rely on expert network pen testers to find hidden flaws that other approaches can't.

Mobile Application Pen Test

Count on excellent results from a curated team of mobile app security experts.

Cloud Pen Test

Identify vulnerabilities unique to cloud environments, all while respecting the shared responsibility approach.

API Pen Test

Test the security of your APIs, withvresults fully integrated with your SDLC, before they ship.

IoT Pen Test

Find cyber-physical vulnerabilities unique to connected devices, from pacemakers to planes.

Get started today: www.bugcrowd.com/get-started