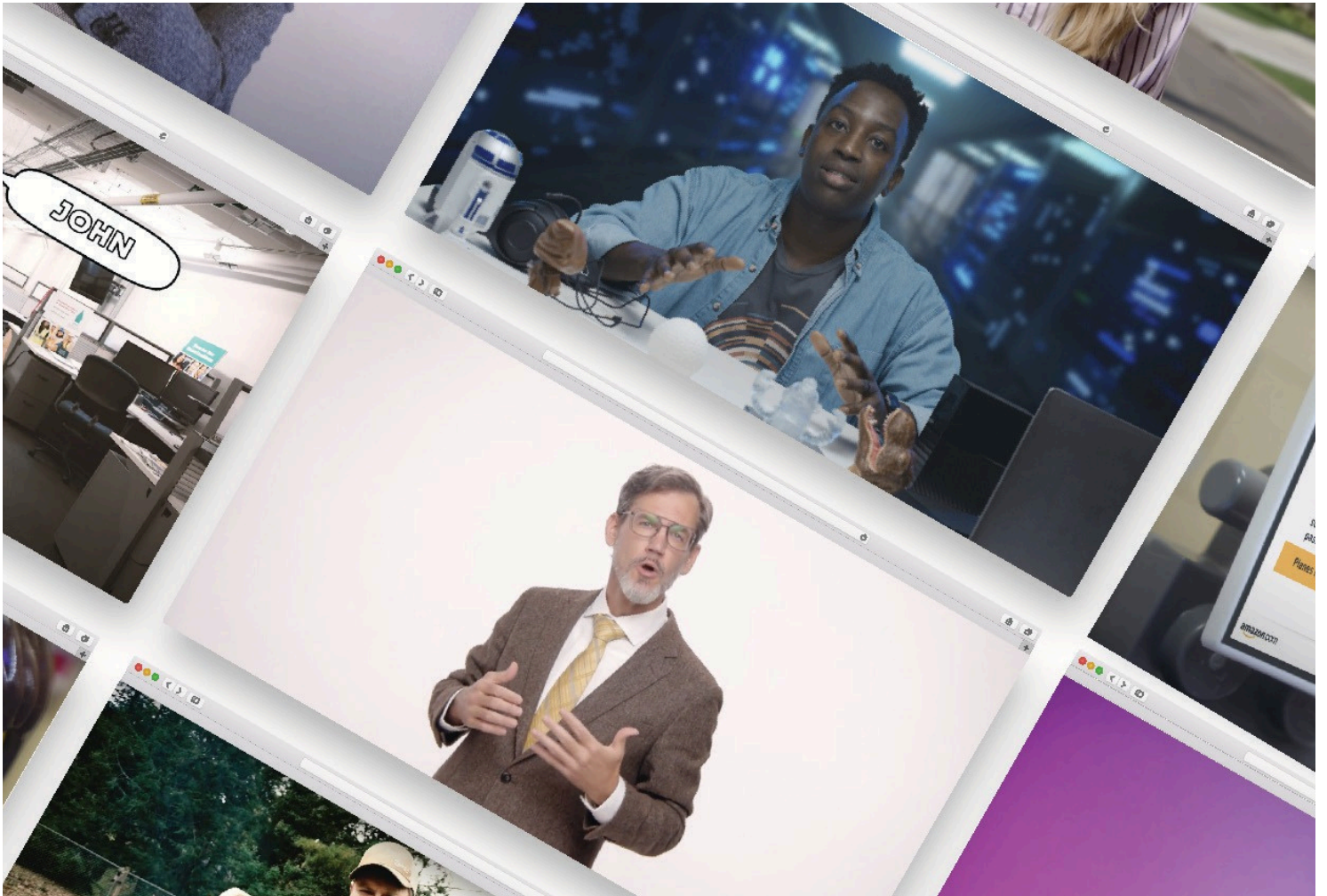


HOOK SECURITY

Hook+

Course Catalog

Spring 2026



WELCOME

A letter from our CEO

Hey. We're really glad you're here.

We started Hook Security because we believed security awareness training could be better, a lot better. Not just better-looking or better-produced, but fundamentally better at the one thing it's supposed to do: actually change how people think and behave.

The old way of doing this wasn't working. Boring slide decks that nobody remembered. "Gotcha" phishing tests that embarrassed people instead of teaching them. Compliance checkboxes that got clicked and forgotten. We'd seen it firsthand, and we were tired of it, so we built something different.

Everything at Hook is built on a simple idea we call PsySec, Psychological Security. It starts with a question most training skips entirely: why do people fall for attacks in the first place? The answer isn't that they're careless or naive. It's that attackers are deliberate. They exploit real human instincts – urgency, trust, authority, curiosity, fear. Our training teaches people to recognize those triggers, understand why they work, and pause before they act. No shame. No scare tactics. Just science-backed learning that actually sticks.

That philosophy shows up in every course in this catalog. You'll find story-driven content, humor, real-world scenarios, and a tone that respects your intelligence. We believe that boring training gets forgotten, and forgotten training doesn't protect anyone. So we've worked hard to make content that employees actually want to engage with – and that shows in our results.

What you're looking at here is a full library of courses covering everything from phishing and ransomware to AI threats, deepfakes, financial scams, compliance tracks, and beyond. It's updated monthly, because the threat landscape doesn't stand still – and neither do we. This is security awareness the way it should have always been: practical, human, and actually effective.

Welcome to Hook. Let's get to work.

Zach Eikenberry
CEO
Hook Security

OUR APPROACH

Psychological Security

PsySec, or Psychological Security, is a revolutionary approach developed by Hook Security that leverages the principles of psychology to enhance cybersecurity awareness. It's built on the understanding that cybersecurity isn't just about technology; it's about people. After all, it's people who use technology, and unfortunately, it's often people who inadvertently create security risks. Our PsySec approach focuses on changing behaviors and mindsets toward cybersecurity. We work to make each employee aware of their role in maintaining security, helping them understand how their actions can either prevent or invite security threats. By tapping into psychological principles, we can influence behaviors, encouraging more secure practices, and building a stronger security culture within your organization. To accomplish this, we work with a number of subject matter experts who stay abreast of the latest security trends and threats to create our training materials. This means you're not getting stale, outdated information, but rather dynamic, current content that keeps your employees engaged and informed.

Next, our in-house production team takes the thorough curriculum and adds unique and comedic storytelling narratives to the content. This ensures that your employees not only get the right information, but information they'll understand and retain. In essence, PsySec is about empowering your employees to become the first line of defense against cyber threats. By making cybersecurity relatable and understandable, we help create an environment where security becomes second nature to everyone in your organization. It's a powerful, proactive, and human-centered approach to tackling today's evolving cybersecurity challenges.



COMPLIANCE

Meeting compliance requirements

Compliance is a crucial aspect of any security awareness training program. At Hook Security, we understand that meeting industry regulations and standards isn't just about ticking boxes; it's about creating a safer, more secure business environment. That being said, it's crucial that we DO check those boxes and help you demonstrate compliance. Our Security Awareness Training program not only helps your employees become more aware of the security risks and best practices but also ensures that your company stays compliant with the ever-evolving regulatory landscape. We've designed our program to align with a long list of compliance standards, including but not limited to: ISO/IEC 27001 & 27002, NIST 800-171 and NIST 800-53, CMMC Maturity Level 3 Target, HIPAA, PCI, DSS, GDPR, COBIT, NERC CIP, FISMA, and many other state and federal regulations.



The training modules are structured to cover the necessary topics required for these standards, such as data protection, password security, phishing awareness, and more. This means that while your employees are learning how to safeguard your business from cyber threats, they're also learning the practices required to maintain regulatory compliance. But we don't stop there. We provide reports and analytics that track the progress of your employees' training, giving you tangible evidence of your company's compliance efforts. These insights can be invaluable during audits, demonstrating to regulators that your organization takes cybersecurity seriously. In essence, Hook Security's Security Awareness Training helps your company maintain a robust security posture while also ensuring that you meet the necessary compliance requirements. It's a win-win situation - promoting both a secure and compliant business environment.

ANNUAL TRAINING

Courses

Our Annual Training courses are once-a-year programs focused on educating employees about important aspects of cybersecurity. They're designed to keep your staff up-to-date with the latest threats, protection strategies, and best practices in the rapidly evolving field of cybersecurity. The aim is not only to enhance the employee's knowledge but also to foster a culture of security within your organization.





JACK IS BACK! CONCRETE JUNGLE

30 Minutes (10 Modules)

Guess who's back from the woods... and wildly unprepared for office life?

After years of peace, pine trees, and chatting with his only "co-worker," a grizzly bear named Ted, Jack is being dragged back into civilization. But this isn't just any return... it's a mission. A mission to get your team fully compliant!

In his most chaotic adventure yet, Jack trades flannel for firewalls as he takes your team on a laugh-filled, lesson-packed journey to cybersecurity greatness. There will be hijinks. There will be bears. And, yeah, you're gonna learn a thing or two.

Key Takeaways:

- Phishing, SMShing & password pitfalls
- Multi-Factor Authentication – why it matters and how to use it
- Malware, spyware, and AI threats that are more real than Ted
- Deepfakes and the wild future of cyber scams

It's a jungle out there. But don't worry, Jack brought the map (and maybe a bear whistle).



Annual Training with Steven

35 Minutes (12 Modules)

Join Steven, your fun and down-to-earth host, as he walks you through the essentials of cybersecurity. In this course, you'll learn how to recognize phishing attempts, avoid scams, and protect your personal data—all while having a few laughs along the way. Steven makes complicated topics like ransomware, social engineering, and securing your devices easy to understand and even enjoyable.

By the end, you'll know exactly how to keep yourself and your organization safe online, all thanks to Steven's helpful tips and relatable style.

Key Takeaways:

- Spot phishing and scam attempts
- Secure your devices and data
- Understand modern cyber threats like ransomware and AI



“Too Late Show” with Kimberly Cain

35 Minutes (12 Modules)

Join Kimberly Cain and her quirky lineup of guests for a late-night talk show-style cybersecurity course! From the sassy AI ChatGPU to wilderness survivalist Wilderness Jack and the ever-arrogant Mr. Password, each episode will make learning about online security a fun and unforgettable experience. Together, they'll tackle social engineering, phishing, malware, and the importance of strong passwords and multi-factor authentication.

Through humor, playful banter, and interactive games (including pies to the face!), this course offers practical tips to help you avoid falling for cyber scams while keeping you entertained.

Key Takeaways:

- Learn to spot phishing, vishing, and SMShing scams.
- Understand how to create secure passphrases and use multi-factor authentication.
- Discover safe web browsing habits and ways to protect against malware.

Who knew cybersecurity could be this fun?



CYBER SECURITY WITH WILDERNESS JACK

25 Minutes (12 Modules)

Our Wilderness Jack Annual Training Course touches on each area of security an employee should know for the year.

In his most important training ever, Jack will lead your employees through all the dangers and pitfalls of cyber attacks. They'll learn to spot and avoid phishing emails, SMSing attacks, and even how to wrangle fellow co-workers into keeping your office in peak cyber protection. The road ahead is fraught with danger, but with Wilderness Jack, your entire organization will be prepared to take on anything those Cyber bullies throw.



PSYSEC ESSENTIALS

25 Minutes (14 Modules)

PsySec Essentials creates a baseline knowledge for your employees and brings new employees up to speed on cybersecurity threats. This annual training course touches on each area of security an employee should know for the year. Your employees will get a comprehensive overview of the latest cybersecurity threats and best practices to counter them.

PsySec Essentials covers a broad range of topics including: Ransomware, Malware, Passwords, Physical Security, Mobile Security, Social Engineering, Vishing, Working Remotely, Removable Media, Incident Reporting, Phishing, and Safe Web Browsing. The course seeks to foster a culture of cybersecurity awareness and vigilance among all members of an organization, thereby reducing the risk of successful cyber attacks. Each module contains a fun, engaging video, graphics to further employee's understanding, tips, tricks, and a quiz at the end to ensure your employees have absorbed what they've learned.



PSYSEC ESSENTIALS INTERNATIONAL

25 Minutes (14 Modules)

PsySec Essentials: International is a multilingual reimaging of our flagship annual training course. In this course, our two hosts cover the same topics that are covered in all our annual training courses, but are translated into several languages, both linguistically and culturally through high-quality dubbing, text translations, and subtitles. We take immense pride in providing training courses in multiple languages with plans to add more in the future. Our aim is not just to cater to diverse global workforces by eliminating language barriers and fostering inclusivity, but also to communicate crucial cybersecurity topics in a culturally relevant manner. We understand that each culture has its unique customs and values, which we strive to incorporate into our multilingual courses. Our foremost priority is to ensure that individuals understand these critical cybersecurity topics in a way that resonates with them and their cultural context.

Partition:

Our Most Ambitious AI Training Yet

Step into Partition, a mind-bending micro course that blends cybersecurity training with the eerie corporate world of Severance. In this surreal and stylish series, employees are trained to separate their digital lives from their personal ones—literally. It's a strange new world where AI, deepfakes, and data privacy collide in ways that feel all too real.

Through cinematic storytelling and sharp humor, Partition walks learners through today's most urgent AI risks:

- Deepfake manipulation and detection
- AI-powered phishing and scams
- Protecting personal data from predictive tech
- Understanding what AI can and can't do
- Staying ahead in a world where machines move fast and humans click faster

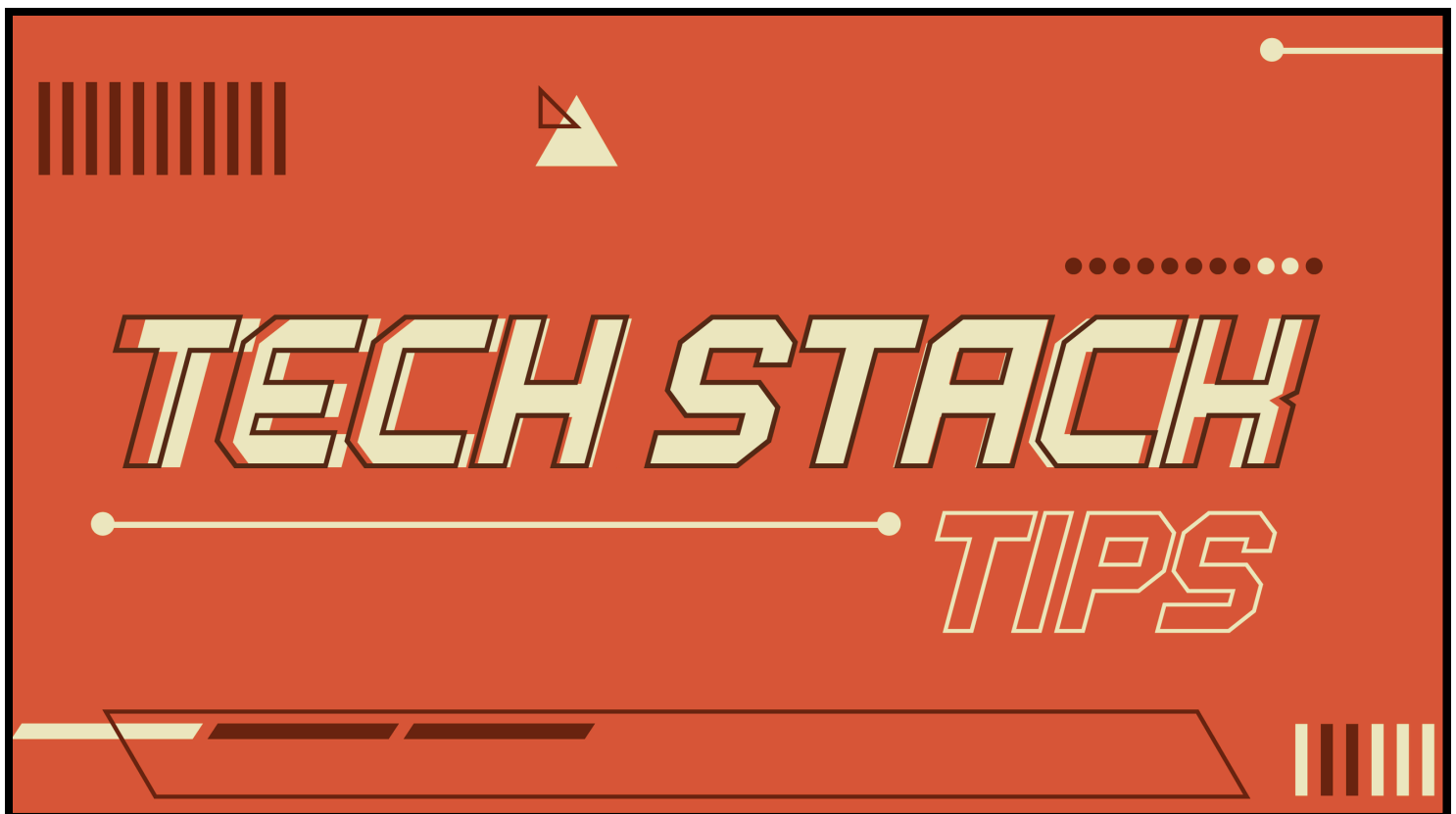
This isn't just another course, it's an experience. Fast, funny, and a little unsettling, Partition helps your team build real awareness in a world that's changing by the second.

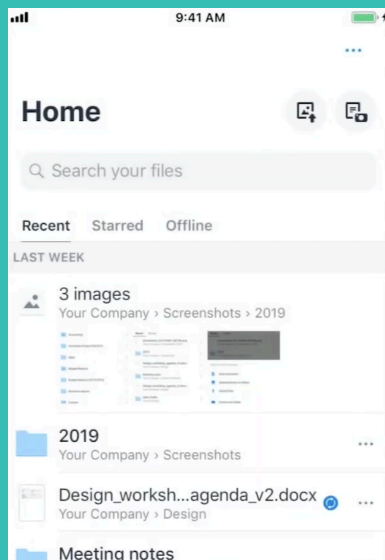


Productivity Training

Courses

Welcome to Hook Security's Productivity Training courses, your go-to resource for empowering employees to maximize efficiency and security. In this section, we focus on Tech Stack Training, providing employees with the skills they need to fully utilize the tools they work with daily. From mastering key features to streamlining workflows, these courses help your team stay productive, reduce downtime, and ensure that security best practices are seamlessly integrated into their everyday routines.





5 Minutes per course (26 total courses)

Welcome to Tech Stack Tips, your go-to series for mastering the tools you use every day! Each of the 26 total courses delivers quick and actionable tips to help you level up your skills with the most popular tech stacks in business today. All around 5 minutes each!

So, Tech Stack Tips has you covered whether you're a tech enthusiast, an IT professional, or just looking to get more out of your apps.

Tech Stack Tips covers ALL of the following software:



MICROLEARNING

Courses

In today's fast-paced world, long training sessions just don't stick. That's why micro training works! These short, focused lessons are delivered right in the flow of work. It's a smarter way to build real security habits.

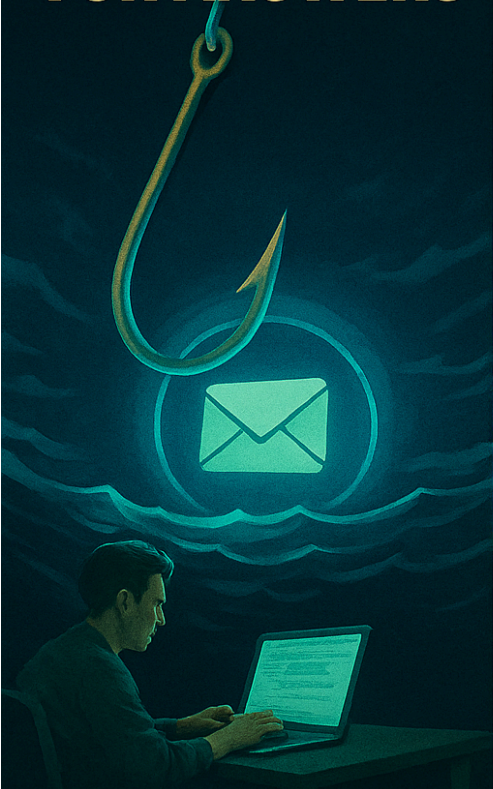
Instead of once-a-year check-the-box training, our micro courses keep your team alert and engaged all year long with bite-sized content that's relevant, flexible, and built for how people actually learn.

Take a look at just a few of our micro courses:

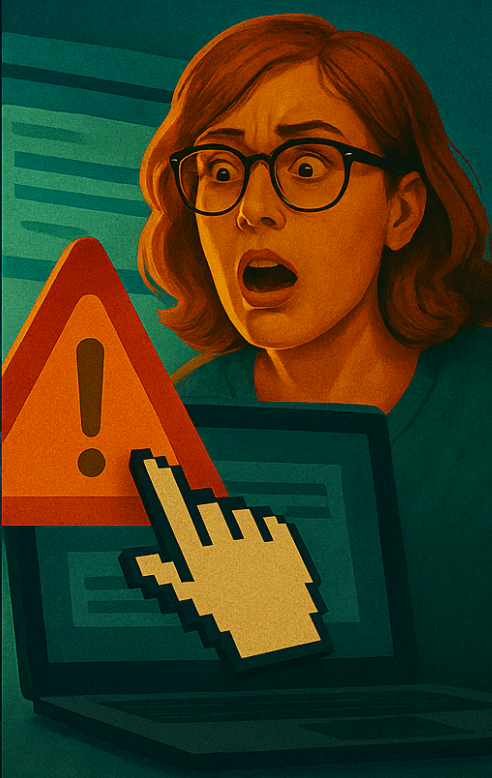
- Phishing for Answers helps employees spot red flags and avoid getting hooked by fake emails.
- Why We Click? digs into the psychology of human behavior, helping your team understand why we fall for scams – and how to stop.
- Corporate Chaos drops learners into a fast-paced scenario where they must respond to real-world security threats in a hectic office environment.

With 20+ micro courses and growing, it's easier than ever to stay sharp, stay secure, and stay compliant – one quick lesson at a time.

PHISHING FOR ANSWERS



WHY WE CLICK?



CORPORATE CHAOS



MICROLEARNING



PHISHING FOR ANSWERS

4-5 Minutes Each Micro Course

These fast-paced lessons walk employees through the most common (and evolving) phishing attacks, teaching them how to:

- Identify suspicious emails and text messages
- Understand social engineering tactics
- Avoid spear phishing, SMSing, and business email compromise (BEC)
- Report phishing attempts before damage is done
-

Whether it's a spoofed sender or a too-good-to-be-true link, this course builds the instincts needed to stay safe.

MICROLEARNING



CORPORATE CHAOS

4-5 Minutes Each Micro Course

This scenario-based course immerses learners in a fictional workplace that's falling apart due to poor security habits. In each short chapter, employees must:

- Make real-time decisions in high-pressure situations
- Spot common security red flags (unlocked screens, lost devices, rogue USBs)
- See how small mistakes create big consequences
- Practice incident response – before the chaos spreads
-

It's fun, fast, and wildly effective at reinforcing day-to-day awareness.

MICROLEARNING



WHY WE CLICK?

4-5 Minutes Each Micro Course

Understanding the why behind our actions is the first step toward changing behavior. This course explores:

- The psychology of urgency, curiosity, and fear
- How scammers exploit human nature
- Real examples of manipulation in everyday messages
- Practical steps to slow down and think before clicking

It's a human-first approach to cybersecurity because awareness starts with self-awareness.

MICROLEARNING



#TRENDING ATTACKS

4-5 Minutes Each Micro Course

Cyber threats don't sit still, and neither should you. This course breaks down the attacks people are falling for right now, so you can spot them before they hit you. No theory. No outdated examples. Just what's working for attackers today.

What you'll see

- Real-world phishing emails that actually get clicks
- Text message scams designed to feel urgent and legit
- QR codes hiding malicious links in plain sight
- Fake voices and AI-generated messages impersonating real people
- Login prompts and "approval" tricks that bypass MFA

What you'll learn

- How to recognize modern attack patterns instantly
- What attackers are counting on you to ignore
- Simple ways to pause, verify, and avoid getting caught
- Why "this looks normal" is exactly the problem

FOREIGN LANGUAGES

Courses

Security training works best when everyone understands it clearly. That's why we offer select courses with subtitles or voiceovers in multiple languages – helping teams stay compliant, no matter where they're located.

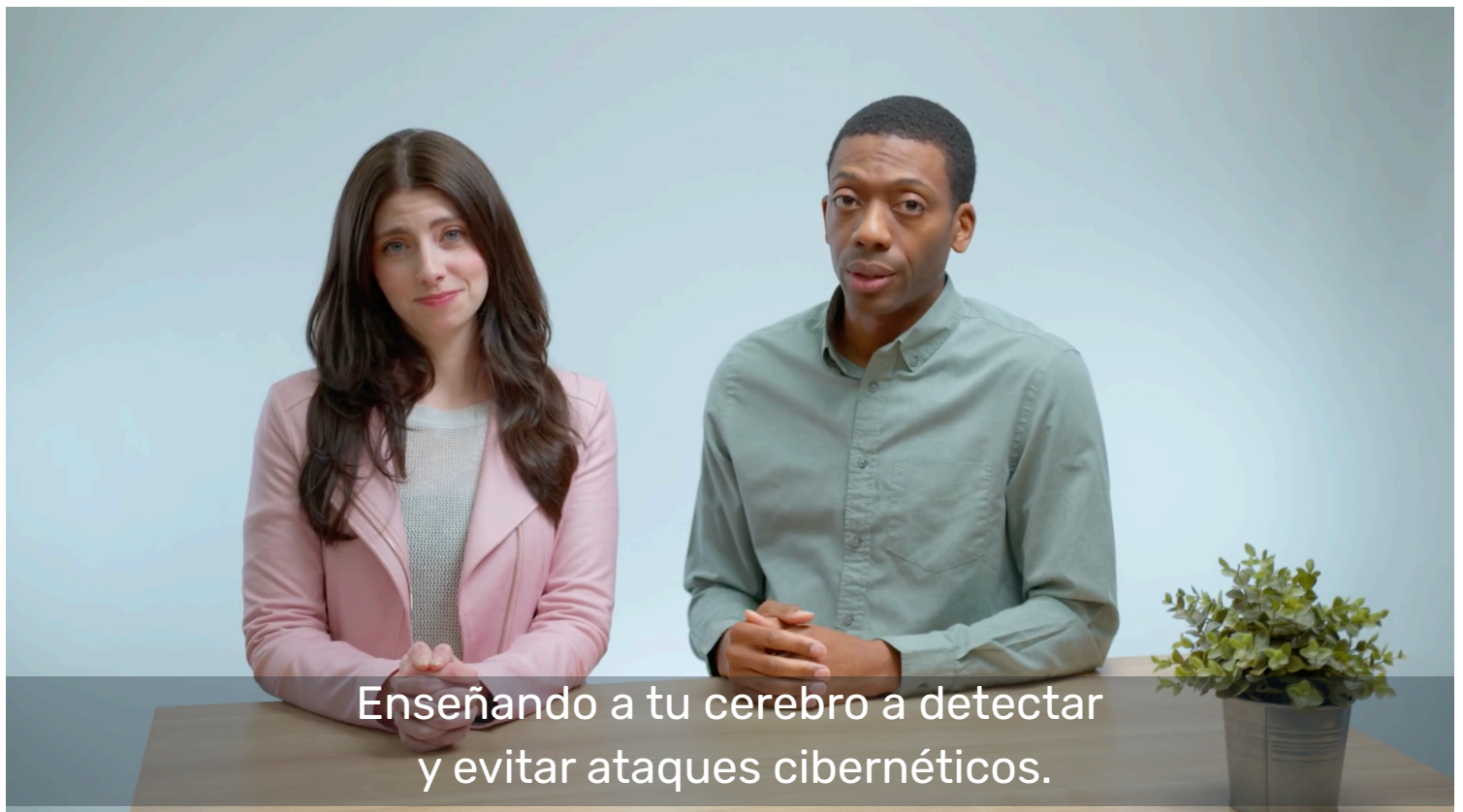
Currently Available:

- Deepfake Course – Subtitles only
 - Czech, German, Spanish, Italian, Portuguese, Turkish, Chinese, Hindi
- Annual Training with Wilderness Jack (Part One) – Spanish (subtitles only)
- PsySec Essentials International – Subtitles + Voiceover
 - German, Spanish, French, French Canadian, Portuguese, Turkish

Need a different course or language?

We can deliver translated versions on demand.

✉ Contact: hello@hooksecurity.co to get started.



Enseñando a tu cerebro a detectar
y evitar ataques cibernéticos.

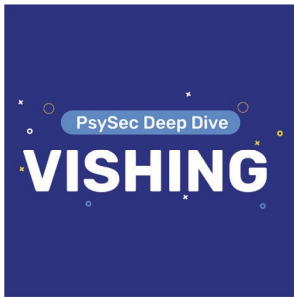
DEEP DIVE

COURSES

13 Courses (4-6 mins each)

Our PsySec Deep Dive series unpacks and explains different subjects in a fun and engaging way. Taking single topics that are often hard to grasp and making them accessible and memorable to all employees. Equipping them with the knowledge and tools they need to stop attacks before they happen.

Each Deep Dive contains a fun, engaging video, graphics to further employees' understanding, tips, tricks, and a quiz at the end to ensure your employees have absorbed what they've learned. This series is great to roll out to employees on a monthly basis to further their knowledge and understanding of these critical cybersecurity topics. Furthering their awareness and reinforcing what they previously learned in their annual training course.



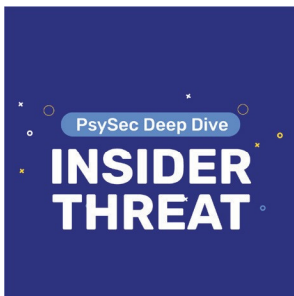
Vishing 10 Minutes

Our Vishing Deep Dive takes an in-depth look at a popular tactic used by cybercriminals called Vishing. With most of today's world owning phones, it's important for employees to learn how to spot and avoid these attacks in order to keep your business's access, information, and data private.



Physical Security 10 Minutes

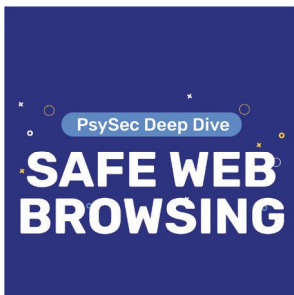
Our Physical Security Deep Dive takes an in-depth look at the physical world around us. While it's common to think of cyberattacks as things like malware and phishing, it's also important to keep in mind the physical security flaws that can put your company at risk. In this Deep Dive, your employees will gain the knowledge needed to keep their devices, information, and data secure from hackers looking to walk into a place and take what doesn't belong to them.



Insider Threat 10 Minutes

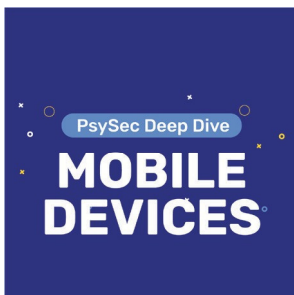
Our Insider Threat Deep Dive takes a closer look at the various types of insider threats that exist, including both malicious and unintentional threats. They will gain insights into the motivations and tactics used by insiders to compromise an organization's security. Covering how to identify potential risk indicators and best practices for mitigating these risks.





Safe Web Browsing 10 Minutes

Our Safe Web Browsing Deep Dive provides employees with a better understanding of various online threats. Diving into the importance of secure connections, malicious websites, the risks associated with downloading content from unverified sources, and more. Guiding employees on the use of security tools, keeping software updated, and providing them the knowledge needed to safely browse the web.



Mobile Devices 10 Minutes

Our Mobile Devices Deep Dive takes an in-depth look at the risks accompanied by owning a mobile device. While these devices are great for keeping us connected, they also hold tons of information about you and your company. This deep dive provides your employees with the knowledge to keep this information and data safe.



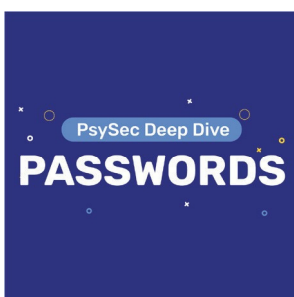
Social Engineering 9 Minutes

Our Social Engineering Deep Dive provides employees with a comprehensive overview of the threats and tactics involved in this type of cyber attack. You will learn how to identify vulnerable targets, craft effective strategies to exploit weaknesses and develop steps to protect yourself from social engineering attacks. By the end of this course, you will have all the skills needed to defend against social engineering attacks.



Malware 10 Minutes

Our Malware Deep Dive takes an in-depth look at the various types of malware out there. This includes viruses, ransomware, spyware, and many more. Employees will gain insight into how malware infects systems, common delivery methods, signs to look out for, preventative measures, and steps to take if they suspect a malware attack.



Passwords 8 Minutes

Our Passwords Deep Dive takes an in-depth look at the importance of keeping our passwords secure. This course also dives deep into learning what types of passwords work and which ones can put your information and data in danger.



Phishing 10 Minutes

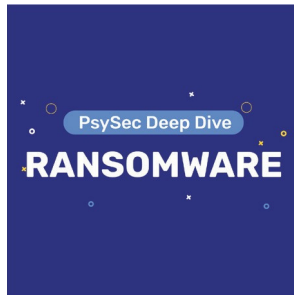
Our Phishing Deep Dive provides an in-depth look at popular phishing tactics cybercriminals are utilizing today. Providing your employees with tips and tricks to look out for in order to spot and avoid this popular attack.



Working Remotely

9 Minutes

In our Working Remotely Deep Dive, employees will learn about the unique cyber security challenges associated with remote work and how to mitigate them effectively. They'll be educated on the importance of secure home networks, the risks associated with public Wi-Fi, and the need for robust passwords and two-factor authentication. Covering best practices when it comes to protecting against potential security vulnerabilities.



Ransomware

10 Minutes

Our Ransomware Deep Dives provide an in-depth look at what ransomware is and looks like. Not only will your employees learn how to spot this vicious attack, but also what to do if they believe they've fallen victim to a ransomware attack.

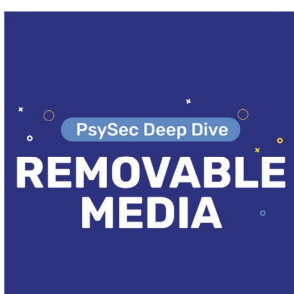
HOW DO YOU STOP RANSOMWARE?



Incident Reporting

8 Minutes

Our Incident Reporting Deep Dive provides an in-depth review of the crucial role employees play in an organization's response to potential cyber threats. They'll be educated on how to recognize signs of a cybersecurity incident, such as unusual system behavior, unauthorized account access, or suspicious emails. This course provides insights into the importance of timely and accurate reporting and how they directly contribute to maintaining your organization's cybersecurity health.



Removable Media

10 Minutes

Using removable media devices, such as USB drives and external hard drives, to gain access and information from your devices is a popular tactic used by cybercriminals. This Deep Dive unpacks this popular scam and provides tips and tricks for avoiding falling victim to this attack.



Mike Fry The Cyber Guy

10 Course (6-8 Minutes Each)

Mike Fry The Cyber Guy is the Bill Nye of cybersecurity. This series adds a new and fun character to our monthly courses, all while diving deep into specific topics from phishing to ransomware, and more. Perfect for reinforcing what employees have learned in our Annual Training Module. Each Mike Fry course contains a fun, engaging video, graphics to further employees' understanding, tips, tricks, and a quiz at the end to ensure your employees have absorbed what they've learned. This is a great series to roll out to users on a monthly basis. Further enhancing their knowledge on important cyber security topics and keeping them engaged.



Working Remotely 8 Minutes

In our Working Remotely course, employees will grasp the unique security challenges that come with remote work environments. The course will explore essential topics such as the importance of securing home networks, potential risks associated with public Wi-Fi, and the need for strong password practices and two-factor authentication. Employees will also learn about how to properly use VPNs to ensure secure connections and how to identify and respond to phishing attempts specifically targeting remote workers.



Social Media Scams 8 Minutes

This Social Media Scams course dives deep into the dangers accompanied by social media, providing employees with examples of popular scams and tips to avoid them. They'll learn best practices for safe social media use, including verifying friend requests and reporting suspected scam activity. By understanding the threats posed by social media scams, employees can safely navigate these platforms and protect both themselves and the organization.



Insider Threat 8 Minutes

In this Insider Threat course, employees will learn about the potential cybersecurity risks that can originate from within the organization. They'll be educated on the various types of insider threats, ranging from unintentional errors made by employees to malicious actions carried out by disgruntled staff or infiltrators. The course aims to equip employees with the knowledge and skills to identify and respond to insider threats, enhancing overall organizational security.



Social Engineering

8 Minutes

In our Social Engineering course, employees will learn about the psychological manipulation techniques used by cybercriminals to trick individuals into revealing confidential information or performing actions that compromise security. They'll be educated on various types of social engineering attacks, including phishing, pretexting, baiting, and tailgating. This knowledge will empower employees to act as the first line of defense against these common yet potentially damaging attacks.



Malware

8 Minutes

In this Malware course, employees will learn about various types of malicious software including viruses, worms, trojans, ransomware, and spyware. They'll grasp how these threats operate, the potential damage they can cause, and the common methods cybercriminals use to distribute them. By understanding how to combat malware, employees can contribute significantly to the organization's cybersecurity efforts.



Passwords

8 Minutes

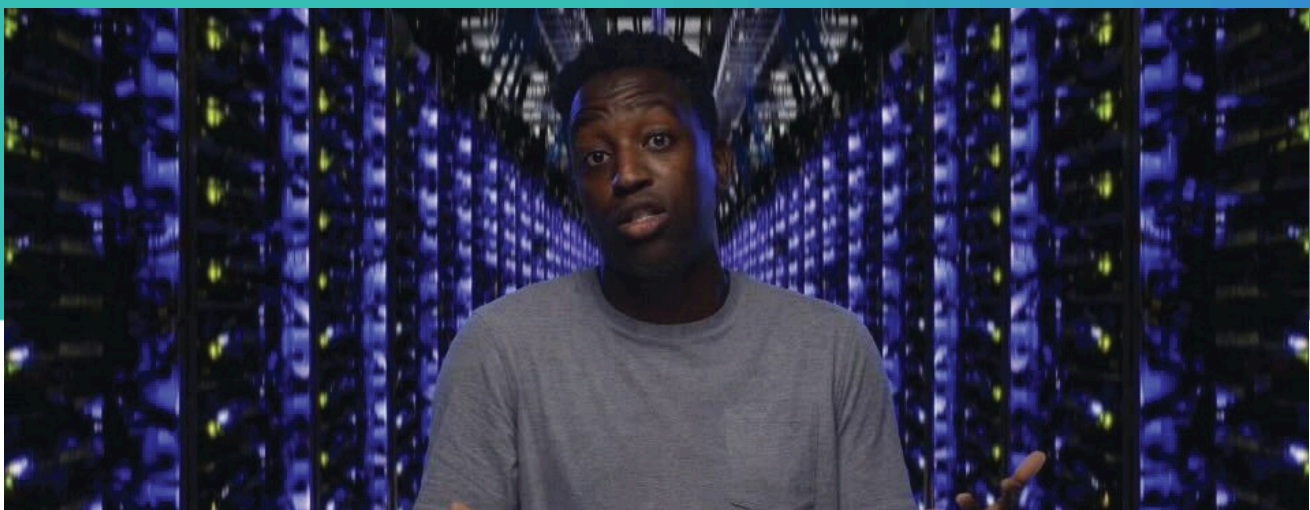
In our Passwords course, employees will learn about the critical role that strong, unique passwords play in protecting personal and organizational data. The course will also cover the risks associated with password reuse and the benefits of using password management tools. Additionally, they'll learn about multi-factor authentication methods and ultimately gain the knowledge to create and manage passwords that effectively safeguard against unauthorized access.



Phishing

8 Minutes

In this Phishing course, employees will learn about one of the most common and dangerous forms of cyber attack. They'll be educated on various types of phishing scams, such as email phishing and spear phishing. The course will teach them how to identify signs of phishing attempts and preventative measures. This knowledge will equip employees with the skills needed to detect and avoid phishing scams, enhancing their own and the organization's cybersecurity.





Update your devices

RANSOMWARE

With Mike Fry the Cyber Guy

Ransomware

8 Minutes

In this Ransomware course, employees will learn about this type of malicious software that encrypts the victim's files and demands a ransom payment to restore access. They'll be educated on how ransomware attacks are typically launched, often through phishing emails or exploiting vulnerabilities in software. The course will teach them how to recognize potential ransomware threats and best practices for avoiding this malicious attack.

MOBILE DEVICES

With Mike Fry the Cyber Guy

Mobile Devices

8 Minutes

In this Mobile Devices course, employees will learn about the unique security challenges associated with smartphones, tablets, and other mobile devices. They'll be educated on various threats such as malware, unsecured Wi-Fi networks, and physical theft or loss of devices. The course will cover how to recognize potential risks and best practices for safeguarding their mobile devices.

SAFE WEB BROWSING

With Mike Fry the Cyber Guy

Safe Web Browsing

8 Minutes

In our Safe Web Browsing course, employees will learn about the potential online threats and how to navigate the internet securely. They'll be educated on various forms of cyber threats including phishing sites and malware-laden downloads. This course will equip employees with the knowledge to browse the web safely, reducing the risk of cyber attacks and protecting sensitive company data.



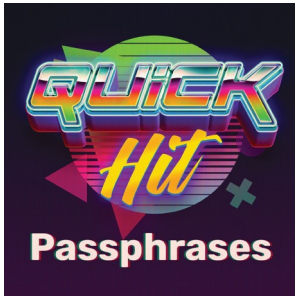
QUICK HITS

12 Course (4 mins each)

The Quick Hits series are short courses that help remind your employees of popular cybersecurity topics while providing quick refreshers. Taking single security topics and promptly highlighting the most important aspects, tips, and tricks. They're perfect for reinforcing what employees have already learned, or providing quick and effective help to employees who are struggling. Each course is accompanied by one to two short, 60 to 90-second videos and a quiz at the end.

Quick Hit courses cover the follow:

- Passphrases
- Vishing
- Social Engineering
- Mobile Devices
- Cyber Security at Home
- Phishing
- Physical Security
- Ransomware
- Malware
- Safe Web Browsing
- Incident Reporting
- Removable Media



Passphrases 2 Minutes

Long gone are the days of using your birthday or dog's name as a password. In this Quick Hit, employees will learn how to change their passwords to a passphrase, how to create one effectively, and how crucial using multi-factor authentication and a password manager is.



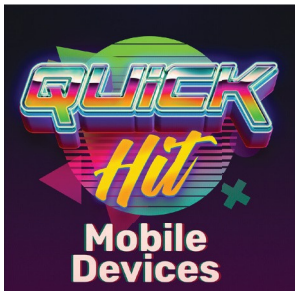
Vishing 3 Minutes

The past couple of years have seen a global rise of cybercrime through various channels. One of them is vishing, which is a term that combines "voice" and the crime of "phishing." In this Quick Hit, we discuss what vishing is, how it's carried out, and ways in which you can spot and avoid these attacks.



Social Engineering 3 Minutes

Even the most technically impenetrable cybersecurity strategy still has one innate flaw: the possibility of human error. This is what cybercriminals that utilize social engineering tactics count on. They prey on and manipulate unsuspecting people into giving their sensitive information. In this Quick Hit, we discuss the four most common types of social engineering attacks.



Mobile Devices 2 Minutes

Our Mobile Device Attacks Quick Hit provides employees with tips and tricks needed to prevent attacks on their mobile devices. As the world becomes more digitally connected, you can rest assured your employees are equipped with the proper knowledge and tools needed to avoid these types of attacks.



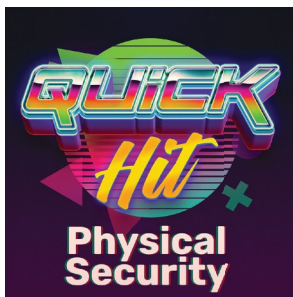
Cyber Security at Home 2 Minutes

While more and more employees are starting to work from home, it's important to teach them how to be cyber-safe at home. Our Cybersecurity at Home Quick Hit provides employees with steps to take to ensure their company's information and data is secure at home.



Phishing 2 Minutes

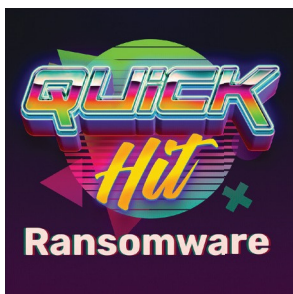
Phishing attacks are one of the oldest forms of cybercrime on the internet, so it's vital your employees understand how these attacks work and how to prevent them. In this Quick Hit, we discuss four of the most common forms of phishing.



Physical Security

2 Minutes

As technology develops, danger can come from anywhere, and physical security becomes critical. In this Quick Hit, we cover what physical security is, how it works, and how you can keep your software and office safe.



Ransomware

2 Minutes

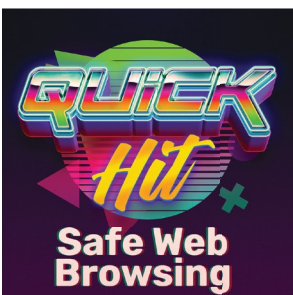
Ransomware has become more prevalent in the past few years, as more and more people have encountered ransomware on their computers. In this Quick Hit, we cover what ransomware is, how it works, and how you can fight against it.



Malware

2 Minutes

Our Malware Quick Hit explains the dangers that come with malware. Not only will your employees learn what malware is, but also the dangers that come along with it, how to spot it, and what to do if one believes their device has been infected.



Safe Web Browsing

2 Minutes

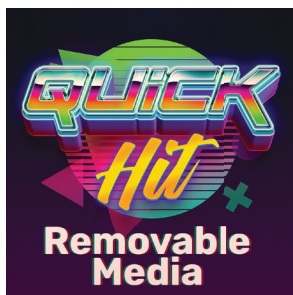
We all know to use our discretion when browsing for information online. But it's so easy to get distracted by links, ads, videos – even your social media feeds, so much so that you could be at risk of becoming exposed to risky content without even realizing it. In this Quick Hit, we cover three tips your employees should follow to browse the web safely.



Incident Reporting

2 Minutes

What should you do when you've fallen victim to a cyber attack? In this Quick Hit, we're discussing the steps you should take to assess and start repairing the damage caused by hacking, phishing, or a ransomware attack.



Removable Media

2 Minutes

Over the years, technology has advanced to allow for more accessible storage of documents and files. However, with every advance in technology come new challenges. In this Quick Hit, we cover ways in which you can keep your portable devices protected.

COMPLIANCE

Courses

Our Cybersecurity Awareness Training meets compliance requirements for various standards, including HIPAA, PCI, and GDPR. However, for these and other specific frameworks, we offer specialized training to ensure your team's understanding of their unique subject matter and additional requirements.





HIPAA

30 Minutes (12 Modules)

Our HIPAA Compliance Training gives employees a HIPAA introduction including how to recognize PHI, proper uses and disclosures of PHI, how to keep PHI secure, and how to report a breach of PHI. Ensuring your employees understand their responsibilities and obligations under the law and helping your organization avoid costly fines and penalties for non-compliance. Our HIPAA training also educates your employees on security best practices, such as password management, secure communication, how to spot and avoid phishing, and other security incidents.

PCI

30 Minutes (12 Modules)

Our PCI compliance course helps train your employees in understanding their obligations in handling payment card data. Helping your organization become PCI compliant and avoiding potential legal liabilities, fines, and penalties for non-compliance. Our PCI compliance training course also educates employees on the importance of protecting payment card data. Providing employees with guidelines on secure data handling practices.



GDPR

30 Minutes (12 Modules)

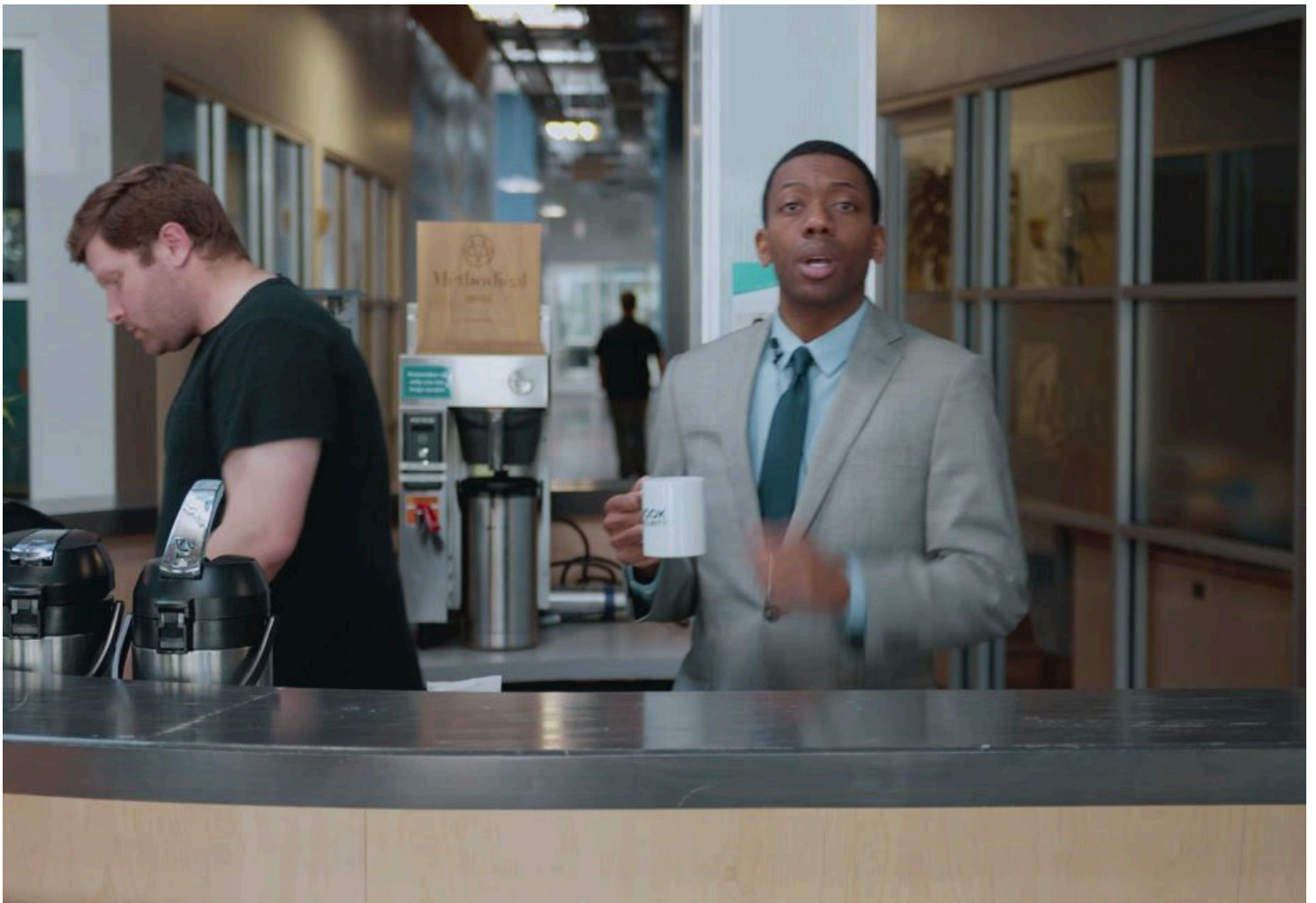
Our GDPR compliance training emphasizes the protection of an individual's personal data and raises awareness to your employees about the importance of safeguarding personal data from unauthorized access, use, or disclosure. Your employees will be educated on best practices for handling personal data, such as types of data, lawful processes, individual rights, data breach protocol, and other privacy incidents.

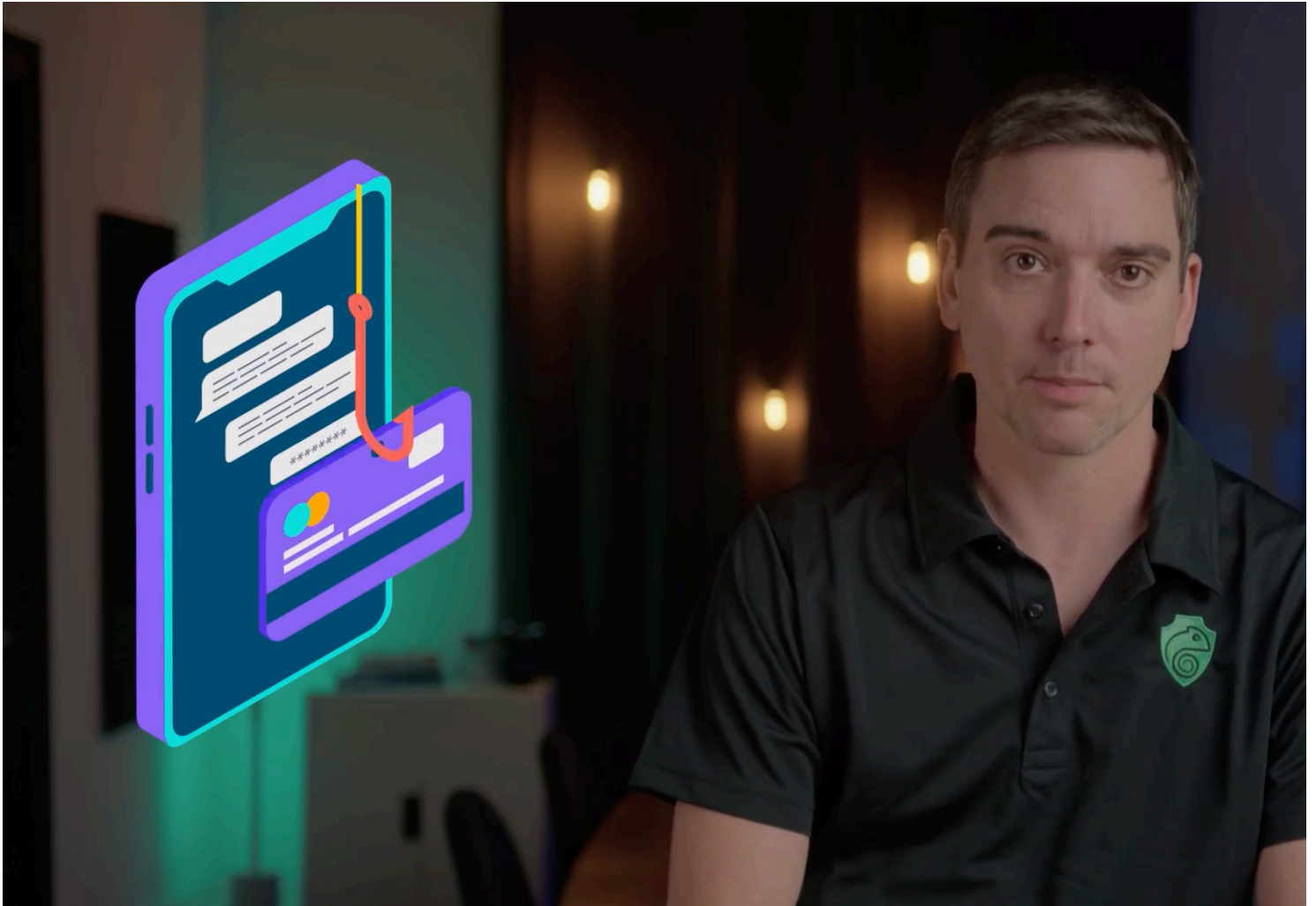


STAND ALONE

Courses

In some cases, companies may see certain cybersecurity issues that need to be addressed more in-depth. These Stand Alone courses are a great way to do so. All the while further educating employees and strengthening your company's defense regarding its cyber security posture. Each course takes a deep dive into a specific topic and takes an in-depth look at popular cybersecurity attacks, best practices, tips, and tricks.





Deep Fakes with Breacher.ai

25 Minutes (9 Modules)

Get ready to dive into one of the most exciting, yet alarming, developments in cybersecurity—Deepfakes. This course, presented by Jason Thatcher, founder of Breacher.ai, in partnership with Hook Security, brings you cutting-edge training on how to recognize and defend against Deepfake threats. Through fun, engaging content, you'll learn how AI-generated videos, audio, and images can be used for social engineering attacks and why you, the employee, are the most important line of defense in this battle.

With real-world examples and expert insights, this course explores the evolution of Deepfakes, how they're created, and the devastating impact they can have on both personal and professional lives. By the end, you'll not only be able to spot Deepfakes but also be armed with the knowledge to protect yourself and your organization. This isn't just cybersecurity—this is the future of fraud, and it's time to stay ahead!



Gone Phishing

18 - 20 Minutes (9 Modules)

This course, "Gone Phishing," follows two people on a fishing excursion. Along the way, your employees will learn about the various forms of phishing attacks and how to identify and respond to them effectively. They'll be educated on common phishing techniques such as deceptive emails, fake websites, and malicious links or attachments. The course will cover how to recognize telltale signs of phishing attempts, including generic greetings, poor grammar, and requests for personal information. Participants will also learn about the potential consequences of falling for phishing scams and how to properly report phishing attempts. Ultimately equipping your employees with the knowledge and skills to safeguard themselves and their organization from phishing threats. Increasing your company's security posture and giving your employees the tools they need to keep your organization safeguarded from potential phishing attacks.



INDUSTRY SPECIFIC

5 - 8 Minutes Per Course (6 Courses)

While cybersecurity is relevant to all companies, some industries face unique cyber threats. From wire fraud in real estate to protecting student data in education, there are certain vulnerabilities that employees in these industries need to be aware of. That's where our Industry Specific Best Practices series comes into play. Our Industry Specific courses include Healthcare, Small Businesses, Higher Education, Law Firms, Financial Institutions, and Real Estate Agencies. Each course includes a fun, engaging video, graphics to further employees understanding, tips, tricks, and a quiz at the end to ensure your employees have absorbed what they've learned. This course series is a great addition to your organization's security efforts and furthering your employees' knowledge on important cybersecurity topics.



SMShing For Answers

12 Minutes (6 Modules)

When it comes to cyber attacks, we all know a good ole phishing email when we see it. But cyber criminals are adaptive and creative. More and more smishing attacks, a form of phishing that involves malicious text messages, are hitting our phones. In our course, SMShing For Answers, employees will learn what smishing is, how it works, and the potential risks involved. This course covers how to identify telltale signs of smishing, such as urgent language, requests for personal information, or links to unfamiliar websites. They'll also be taught how to respond appropriately to suspected smishing attempts, including not responding to the message, never clicking on embedded links, and reporting the incident. Ultimately empowering your employees with the knowledge needed to protect themselves and their organizations from smishing threats.



MULTI-FACTOR AUTHENTICATION

18 Minutes (5 Modules)

In our Multi-factor Authentication (MFA) course, your employees will learn about the importance and implementation of MFA as an essential line of defense in securing online accounts. The course will explain what MFA is, and help employees understand the different types of authentication factors, such as something you know (password), something you have (smartphone), and something you are (biometrics). They'll be guided on how to set up MFA on various platforms and taught about potential threats that MFA helps to mitigate, like brute force attacks and credential stuffing. Importantly, your employees will gain an understanding of why relying solely on passwords is insufficient in today's cybersecurity landscape.

INSTANT TRAINING

For Phishing Simulations

In addition to the courses that are consumed through enrollments via our LMS, Hook Security also provides “Instant Training” which is shown when an employee fails a phishing simulation. Instant Training instantly trains your employees as soon as they click on a phishing simulation. They’ll see a landing page with a video that highlights what they missed and what to look out for in the future. This just-in-time, non-punitive approach helps create good habits and attitudes around cybersecurity that reduces click rates over time. In our content library, you’ll find options for generic instant training videos, which can be applied to the thousands of phishing templates provided, as well as a selection of premium instant training videos that enhance the teachable moment experience.





The Click Report

Universal Training Videos

The original Click Report that started it all. These quick, focused training videos help employees recognize the most common red flags found in phishing emails before those emails become real problems.

When an employee clicks on a phishing simulation, they're immediately redirected to a landing page that explains what happened and why the message was suspicious. From there, they'll watch a short Click Report video that breaks down the specific red flags they missed and shows them what to look for next time. Each video focuses on one of the most common phishing tactics attackers use, things like brand impersonation, "too good to be true" offers, urgent requests, scare tactics, and other psychological triggers designed to get people to click first and think later.

Because each video is tied to a specific phishing red flag, you can easily pair it with any of the thousands of phishing templates available in the platform. The result is simple, relevant training that meets employees in the exact moment they need it most, right after a simulated mistake, turning a click into a learning opportunity.



The Click Report Premium

The Click Report Premium takes phishing training a step further by turning each simulated attack into a guided investigation. Instead of focusing on just one red flag, these videos break down the entire phishing email—showing employees multiple warning signs they may have missed and explaining how attackers design messages to trick people into clicking.

When an employee clicks on a phishing simulation, they're redirected to a landing page that reveals the test and launches a Click Report Premium video. From there, the video walks through the phishing email piece by piece, highlighting suspicious elements such as spoofed brands, unusual sender addresses, urgent language, suspicious links, and other common attacker tactics.

Because these videos analyze the full email rather than just a single red flag, they provide deeper context and a more complete learning experience. Employees begin to understand not just what they missed, but how phishing emails are constructed and why they can be so convincing.

The result is a more immersive training moment that helps employees build stronger instincts for spotting phishing attacks in the real world—turning a simulated mistake into a meaningful learning experience.

Hook+ Catalog

V 3.2