mimecast awareness training actors

mimecast awareness training actors are a pivotal element within the Mimecast Awareness Training platform, designed to elevate cybersecurity knowledge and behavior in organizations. This article explores who these actors are, their roles in delivering engaging security awareness content, and how their performances enhance user retention. Readers will gain insight into how Mimecast utilizes professional actors to present real-world scenarios, why this approach is effective, and how it supports ongoing cybersecurity education. Additionally, the discussion covers the production process, the feedback received from organizations, and best practices for optimizing awareness training participation. Whether you're a security professional or part of an HR team, understanding the impact and methodology of mimecast awareness training actors will help you maximize the value of your cyber awareness initiatives.

Understanding Mimecast Awareness Training Actors

Mimecast awareness training actors are skilled professionals featured in the Mimecast cyber awareness modules. Their primary role is to bring to life various cybersecurity scenarios, making the training more relatable and memorable for employees. By portraying realistic workplace situations, these actors demonstrate both secure and insecure behaviors, helping learners recognize threats such as phishing, social engineering, and data breaches. This approach transforms traditional, text-heavy training into dynamic, engaging content that resonates with diverse audiences.

Mimecast’s strategy emphasizes behavioral change through storytelling. The actors serve as visual guides, allowing users to see the consequences of security lapses and the benefits of best practices. This innovative use of professional actors distinguishes Mimecast Awareness Training from many other platforms that rely solely on graphics or animations.

Role and Importance of Actors in Security Training

Why Use Professional Actors in Cybersecurity Education?

Professional actors are integral to effective cybersecurity training because they can convey complex messages in a compelling, human-centered manner. Mimecast awareness training actors utilize their craft to foster emotional connections with viewers, making abstract cyber risks tangible and actionable. Their performances encourage empathy, personal responsibility, and proactive security behavior.

Key Benefits of Actor-Led Training Modules

- Increased learner engagement and attention
- Improved retention of security concepts
- Greater relatability and understanding of workplace scenarios
- Enhanced demonstration of positive and negative security behaviors
- Facilitation of behavioral change through storytelling

Mimecast awareness training actors help bridge the gap between theoretical knowledge and practical application, ensuring that security awareness is not only learned but adopted throughout the organization.

How Mimecast Chooses and Utilizes Professional Actors

Selection Criteria for Mimecast Awareness Training Actors

Mimecast employs a rigorous casting process to select actors who can authentically represent everyday workplace professionals. Selection criteria include acting experience, diversity, relatability, and the ability to deliver educational content with clarity and charisma. Mimecast seeks individuals who can portray a range of personalities, from cautious employees to those who unknowingly fall prey to cyber threats.

Integration of Actors into Training Content

Once selected, actors participate in carefully scripted scenarios developed by cybersecurity experts and instructional designers. These scenarios simulate realistic events such as suspicious emails, password mishandling, or social engineering attempts. Mimecast awareness training actors rehearse and perform these scripts, which are then professionally filmed and edited for maximum impact.

Impact on Learner Engagement and Retention

How Actor-Led Training Improves Learning Outcomes

Research demonstrates that people retain information better when it is presented in a narrative format, especially when delivered by relatable characters. Mimecast awareness training actors play a crucial role in making cybersecurity content memorable and actionable. Their performances help users visualize threats and solutions, increasing the likelihood that best practices will be remembered and applied in real-world situations.

Measuring Engagement and Effectiveness

Organizations that deploy Mimecast Awareness Training often track completion rates, quiz scores, and incident reductions to assess program success. Feedback consistently shows that actor-led modules achieve higher engagement and completion rates compared to traditional, text-based training.

Production Quality and Scenario Authenticity

High-Quality Video Production Standards

Mimecast invests in professional-grade video production to ensure that awareness training modules look and feel polished. The use of quality lighting, sound, and editing techniques enhances the viewing experience, helping maintain user attention throughout each module.

Realistic Scenario Development

Mimecast awareness training actors work with cybersecurity professionals and instructional designers to ensure that each scenario mirrors actual workplace challenges. Scenarios cover a broad spectrum of threats, from phishing attacks to physical security breaches, making the training relevant for employees across departments and industries.

Feedback from Users and Organizations

Employee Reactions to Actor-Led Training

User feedback reveals that employees appreciate the engaging and relatable nature of Mimecast’s actor-led modules. Many report finding the content more enjoyable and easier to understand than traditional training formats. The presence of mimecast awareness training actors helps reduce resistance to mandatory training by providing a more entertaining and practical experience.

Organizational Outcomes and Case Studies

Organizations leveraging Mimecast awareness training actors often observe measurable improvements in security culture. Case studies highlight reduced phishing click rates, increased reporting of suspicious activity, and sustained behavioral change over time. Security teams also report that actor-led modules foster more meaningful discussions about cybersecurity risks and solutions.

Best Practices for Maximizing Training Effectiveness

Strategies for Successful Implementation

To maximize the impact of mimecast awareness training actors, organizations should adopt a structured approach to deployment. This includes scheduling regular training intervals, encouraging open dialogue about scenarios, and integrating training modules with other security initiatives.

Tips for Increasing Participation and Retention

1. Promote training as a vital part of professional development
2. Recognize and reward participation and completion
3. Customize training schedules to suit departmental workflows
4. Facilitate post-training discussions and feedback sessions
5. Monitor and act on training data to identify areas for improvement

By following these best practices, organizations can ensure that mimecast awareness training actors deliver maximum value and foster a stronger culture of cyber resilience.

Conclusion

Mimecast awareness training actors are a cornerstone of Mimecast’s approach to cybersecurity education. Their involvement transforms routine training into an engaging, memorable experience. Through professional performances, realistic scenarios, and high-quality production, Mimecast enables organizations to build lasting security awareness and foster behavioral change. By understanding the role and impact of mimecast awareness training actors, organizations can leverage this innovative approach to strengthen their defense against evolving cyber threats.

Q: What are mimecast awareness training actors?

A: Mimecast awareness training actors are professional performers featured in Mimecast’s cybersecurity training modules. They portray realistic workplace scenarios to help employees recognize and respond to security threats.

Q: How do mimecast awareness training actors improve engagement?

A: Actors make training more engaging by presenting relatable situations and behaviors, which helps learners connect emotionally and retain information more effectively than traditional text-based modules.

Q: What types of scenarios do mimecast awareness training actors perform?

A: Mimecast awareness training actors perform a range of scenarios, including phishing attacks, password mishandling, social engineering attempts, and physical security breaches, all designed to mirror real workplace challenges.

Q: Why does Mimecast use professional actors instead of animations?

A: Professional actors bring authenticity and relatability to training modules, making security concepts easier to understand and remember. Their performances foster behavioral change by demonstrating real-life consequences.

Q: How are mimecast awareness training actors selected?

A: Mimecast selects actors based on their experience, relatability, diversity, and ability to communicate educational content clearly and engagingly. A rigorous casting process ensures the right fit for each scenario.

Q: What feedback do organizations give about actor-led training?

A: Organizations report higher engagement, improved retention rates, and measurable behavioral change among employees after implementing actor-led Mimecast Awareness Training modules.

Q: Can mimecast awareness training actors help reduce security incidents?

A: Yes, organizations often see a reduction in phishing click rates and an increase in the reporting of suspicious activities after deploying actor-led training, indicating improved security awareness.

Q: Are mimecast awareness training modules customizable?

A: Mimecast offers flexibility in scheduling and module selection, allowing organizations to tailor training content to different departments and risk profiles.

Q: How often should organizations use mimecast awareness training actors in their programs?

A: Regular, ongoing training intervals—such as monthly or quarterly—help reinforce security concepts and maintain high levels of awareness throughout the organization.

Q: What makes mimecast awareness training actors different from other cyber awareness solutions?

A: Mimecast stands out by using professional actors to deliver high-quality, realistic scenarios that drive engagement and behavioral change, setting it apart from platforms that rely solely on static graphics or animations.

Mimecast Awareness Training Actors

Mimecast Awareness Training Actors: Elevating Your Cybersecurity Posture Through Engaging Role-Playing

Introduction:

In today's digitally driven world, cybersecurity threats are more sophisticated and pervasive than ever before. Phishing attacks, ransomware, and malware are constantly evolving, demanding a proactive and engaged workforce to mitigate risks. Mimecast awareness training, often incorporating realistic scenarios and engaging role-playing, plays a crucial role in bolstering your organization's security posture. This post delves into the effectiveness of Mimecast awareness training that utilizes "actors" – individuals or simulated personas – to create impactful and memorable learning experiences. We'll explore how these actors enhance training efficacy, discuss the different approaches employed, and offer insights into optimizing your program for maximum impact.

Why Mimecast Awareness Training Needs Actors (Or

Simulated Actors): The Power of Immersive Learning

Traditional cybersecurity training often relies on static materials like videos and presentations. While informative, these methods can lack the engagement necessary for lasting impact. Mimecast awareness training, when integrated with actors or simulated actors (through interactive modules), significantly improves retention and knowledge application. This immersive approach places learners directly into realistic scenarios, fostering a deeper understanding of potential threats and the best responses.

Instead of passively absorbing information, users actively participate, making decisions with real-world consequences (within the simulation). This active learning drastically increases the likelihood of remembering crucial cybersecurity protocols and reacting appropriately when faced with a genuine threat.

Different Approaches to Utilizing Actors in Mimecast Training

Mimecast doesn't directly provide actors for training; rather, it offers a platform to deliver engaging cybersecurity awareness training. The use of "actors" can be implemented in several ways:

1. Human Actors in Simulated Scenarios: This approach involves employing actors to conduct live role-playing exercises or workshops. These actors might portray phishing scammers, disgruntled employees, or other potential threats, presenting realistic scenarios and testing users' responses. This offers highly interactive and memorable training, but it comes with logistical and financial considerations.

2. Simulated Actors in Interactive Modules: Mimecast's platform enables the creation of sophisticated interactive modules. These modules leverage simulated actors or AI-driven characters to guide learners through different scenarios. Users interact with these simulated actors through text, voice, or video, responding to their actions and choosing different responses. This approach is more cost-effective and scalable than employing human actors.

3. Video-Based Scenarios with Professional Actors: Pre-recorded videos featuring professional actors can create highly engaging scenarios. These videos can effectively demonstrate phishing techniques, social engineering tactics, and other cybersecurity threats. The videos can be incorporated into Mimecast's training modules to provide a visual and engaging learning experience.

Choosing the Right Approach for Your Organization

The optimal approach depends on your organization's budget, resources, and training objectives. For smaller organizations, the cost-effectiveness of simulated actors within interactive modules might be more appropriate. Larger enterprises with greater resources might find that incorporating human actors into live training exercises provides more impactful and immersive experiences.

Measuring the Success of Your Mimecast Awareness Training with Actors

The effectiveness of your Mimecast awareness training with actors needs careful measurement. Key metrics include:

Completion rates: Track the percentage of employees who complete the training program.
Knowledge retention: Assess employee knowledge of cybersecurity best practices through quizzes or simulations after the training.
Behavioral changes: Observe whether employees demonstrate improved cybersecurity habits after completing the training, such as increased caution with suspicious emails.
Phishing simulation results: Conduct regular phishing simulations to gauge the effectiveness of the training in preventing successful phishing attacks.

Optimizing Your Mimecast Awareness Training Program

To optimize your program, consider these tips:

Regular updates: Keep your training materials current with the latest threats and vulnerabilities.
Personalized learning: Tailor the training to the specific roles and responsibilities of your employees.
Gamification: Incorporate game mechanics like points, badges, and leaderboards to increase engagement.
Feedback and iteration: Regularly solicit feedback from employees and use it to refine your training program.

Conclusion:

Mimecast awareness training, augmented with actors or simulated actors, offers a powerful approach to strengthening your organization's cybersecurity defenses. By creating immersive and engaging learning experiences, you can cultivate a security-conscious workforce capable of identifying and responding to threats effectively. Remember to carefully choose your approach, measure your results, and continuously optimize your program to ensure lasting impact. Investing in high-quality awareness training is a vital step in minimizing your organization's risk in the ever-evolving threat landscape.

FAQs:

1. Are there specific Mimecast modules that utilize actors? While Mimecast doesn't explicitly market modules with human actors, many of their interactive modules utilize simulated actors or realistic scenarios presented in engaging ways to achieve similar effect. You should check Mimecast's updated module library.

2. How much does incorporating human actors into Mimecast training cost? The cost will vary significantly based on the number of actors, the duration of the training, and the actors' experience.

It’s a significant investment compared to using simulated actors.

3. Can I integrate external training materials with my Mimecast platform? Mimecast offers integration options; however, compatibility depends on the format and technical specifications of the external materials. Consult Mimecast's documentation or support team.

4. How often should I update my Mimecast awareness training content? Ideally, you should update your training content at least quarterly to keep pace with evolving threat landscapes. More frequent updates are even better.

5. What metrics beyond completion rates should I track to measure success? Track knowledge retention via post-training assessments, analyze phishing simulation results, and observe changes in user behavior to gain a holistic view of training effectiveness.

mimecast awareness training actors: Network Security Strategies Aditya Mukherjee, 2020-11-06 Build a resilient network and prevent advanced cyber attacks and breaches Key Features Explore modern cybersecurity techniques to protect your networks from ever-evolving cyber threats Prevent cyber attacks by using robust cybersecurity strategies Unlock the secrets of network security Book Description With advanced cyber attacks severely impacting industry giants and the constantly evolving threat landscape, organizations are adopting complex systems to maintain robust and secure environments. Network Security Strategies will help you get well-versed with the tools and techniques required to protect any network environment against modern cyber threats. You'll understand how to identify security vulnerabilities across the network and how to effectively use a variety of network security techniques and platforms. Next, the book will show you how to design a robust network that provides top-notch security to protect against traditional and new evolving attacks. With the help of detailed solutions and explanations, you'll be able to monitor networks skillfully and identify potential risks. Finally, the book will cover topics relating to thought leadership and the management aspects of network security. By the end of this network security book, you'll be well-versed in defending your network from threats and be able to consistently maintain operational efficiency, security, and privacy in your environment. What you will learn Understand network security essentials, including concepts, mechanisms, and solutions to implement secure networks Get to grips with setting up and threat monitoring cloud and wireless networks Defend your network against emerging cyber threats in 2020 Discover tools, frameworks, and best practices for network penetration testing Understand digital forensics to enhance your network security skills Adopt a proactive approach to stay ahead in network security Who this book is for This book is for anyone looking to explore information security, privacy, malware, and cyber threats. Security experts who want to enhance their skill set will also find this book useful. A prior understanding of cyber threats and information security will help you understand the key concepts covered in the book more effectively.

mimecast awareness training actors: The Great Reboot Bob Zukis, Paul Ferrillo, Chris Veltsos, 2020-06

mimecast awareness training actors: Essentials of Business Communication Mary Ellen Guffey, 2004 This text-workbook is a streamlined, no-nonsense approach to business communication. It takes a three-in-one approach: (1) text, (2) practical workbook, and (3) self-teaching grammar/mechanics handbook. The chapters reinforce basic writing skills, then apply these skills to a variety of memos, letters, reports, and resumes. This new edition features increased coverage of contemporary business communication issues including oral communication, electronic forms of communication, diversity and ethics.

mimecast awareness training actors: Certified Ethical Hacker Rob Botwright, 101-01-01 □ Dive into the world of cybersecurity with the ultimate Certified Ethical Hacker book bundle! □

Master the art of ethical hacking and fortify your defenses against modern cyber threats with four essential volumes: **Foundations of Ethical Hacking: Understanding Cybersecurity Basics** Build a solid foundation in cybersecurity principles, ethical hacking methodologies, and proactive defense strategies. Perfect for beginners and seasoned professionals alike. **Mastering Session Hijacking: Advanced Techniques and Defense Strategies** Explore advanced session manipulation techniques and learn how to defend against sophisticated session hijacking attacks. Essential for securing web applications and protecting user sessions. **Advanced SQL Injection Defense: Techniques for Security Professionals** Equip yourself with advanced techniques to detect, prevent, and mitigate SQL injection vulnerabilities. Essential reading for security professionals responsible for safeguarding databases. **Cryptography in Cloud Computing: Protecting Data in Virtual Environments** Learn how to secure sensitive data in cloud infrastructures using cryptographic protocols and encryption techniques. Ensure data confidentiality, integrity, and regulatory compliance in virtualized environments. Each book is authored by cybersecurity experts, offering practical insights, real-world examples, and hands-on exercises to enhance your cybersecurity skills. Whether you're preparing for certification exams or advancing your career in cybersecurity, this bundle provides the knowledge and tools you need to excel. Take the next step in your cybersecurity journey and become a Certified Ethical Hacker. Embrace ethical hacking practices, defend against cyber threats, and secure digital assets with confidence. Don't miss out on this exclusive bundle! Secure your copy today and embark on a transformative learning experience in cybersecurity. Equip yourself with the expertise to protect against evolving cyber threats and contribute to a safer digital world. Are you ready to hack ethically and safeguard the future of digital security? Order now and join the ranks of Certified Ethical Hackers worldwide!

mimecast awareness training actors: *Cyber Risk Leaders* Tan, Shamane, 2019 Cyber Risk Leaders: Global C-Suite Insights - Leadership and Influence in the Cyber Age', by Shamane Tan - explores the art of communicating with executives, tips on navigating through corporate challenges, and reveals what the C-Suite looks for in professional partners. For those who are interested in learning from top industry leaders, or an aspiring or current CISO, this book is gold for your career. It's the go-to book and your CISO kit for the season.

mimecast awareness training actors: The Art of Invisibility Kevin Mitnick, 2019-09-10 Real-world advice on how to be invisible online from the FBI's most-wanted hacker (Wired) Your every step online is being tracked and stored, and your identity easily stolen. Big companies and big governments want to know and exploit what you do, and privacy is a luxury few can afford or understand. In this explosive yet practical book, computer-security expert Kevin Mitnick uses true-life stories to show exactly what is happening without your knowledge, and teaches you the art of invisibility: online and everyday tactics to protect you and your family, using easy step-by-step instructions. Reading this book, you will learn everything from password protection and smart Wi-Fi usage to advanced techniques designed to maximize your anonymity. Invisibility isn't just for superheroes--privacy is a power you deserve and need in the age of Big Brother and Big Data.

mimecast awareness training actors: Insider Threat Julie Mehan, 2016-09-20 Every type of organization is vulnerable to insider abuse, errors, and malicious attacks: Grant anyone access to a system and you automatically introduce a vulnerability. Insiders can be current or former employees, contractors, or other business partners who have been granted authorized access to networks, systems, or data, and all of them can bypass security measures through legitimate means. Insider Threat – A Guide to Understanding, Detecting, and Defending Against the Enemy from Within shows how a security culture based on international best practice can help mitigate the insider threat, providing short-term quick fixes and long-term solutions that can be applied as part of an effective insider threat program. Read this book to learn the seven organizational characteristics common to insider threat victims; the ten stages of a malicious attack; the ten steps of a successful insider threat program; and the construction of a three-tier security culture, encompassing artefacts, values, and shared assumptions. Perhaps most importantly, it also sets out what not to do, listing a set of worst practices that should be avoided. About the author Dr Julie Mehan is the founder and

president of JEMStone Strategies and a principal in a strategic consulting firm in Virginia. She has delivered cybersecurity and related privacy services to senior commercial, Department of Defense, and federal government clients. Dr Mehan is also an associate professor at the University of Maryland University College, specializing in courses in cybersecurity, cyberterror, IT in organizations, and ethics in an Internet society

mimecast awareness training actors: Theatrum Arbitri C. Panayotakis, 2018-07-17 Theatrum Arbitri is a literary study dealing with the possible influence of Roman comic drama (comedies of Plautus and Terence, theatre of the Greek and Roman mimes, and fabula Atellana) on the surviving fragments of Petronius' Satyrica. The theatrical assessment of this novel is carried out at the levels of plot-construction, characterization, language, and reading of the text as if it were the narrative equivalent of a farcical staged piece with the theatrical structure of a play produced before an audience. The analysis follows the order of each of the scenes in the novel. The reader will also find a brief general commentary on the less discussed scenes of the Satyrica, and a comprehensive account of the theatre of the mimes and its main features.

mimecast awareness training actors: Ransomware Revealed Nihad A. Hassan, 2019-11-06 Know how to mitigate and handle ransomware attacks via the essential cybersecurity training in this book so you can stop attacks before they happen. Learn the types of ransomware, distribution methods, internal structure, families (variants), defense strategies, recovery methods, and legal issues related to reporting ransomware incidents to authorities and other affected parties. This book also teaches you how to develop a ransomware incident response plan to minimize ransomware damage and recover normal operations quickly. Ransomware is a category of malware that can encrypt your computer and mobile device files until you pay a ransom to unlock them. Ransomware attacks are considered the most prevalent cybersecurity threats today—the number of new ransomware variants has grown 30-fold since 2015 and they currently account for roughly 40% of all spam messages. Attacks have increased in occurrence from one every 40 seconds to one every 14 seconds. Government and private corporations are targets. Despite the security controls set by organizations to protect their digital assets, ransomware is still dominating the world of security and will continue to do so in the future. Ransomware Revealed discusses the steps to follow if a ransomware infection occurs, such as how to pay the ransom through anonymous payment methods, perform a backup and restore your affected files, and search online to find a decryption tool to unlock (decrypt) your files for free. Mitigation steps are discussed in depth for both endpoint devices and network systems. What You Will Learn Be aware of how ransomware infects your system Comprehend ransomware components in simple terms Recognize the different types of ransomware familiesIdentify the attack vectors employed by ransomware to infect computer systemsKnow how to prevent ransomware attacks from successfully comprising your system and network (i.e., mitigation strategies) Know what to do if a successful ransomware infection takes place Understand how to pay the ransom as well as the pros and cons of paying Set up a ransomware response plan to recover from such attacks Who This Book Is For Those who do not specialize in the cybersecurity field (but have adequate IT skills) and want to fully understand the anatomy of ransomware threats. Although most of the book's content will be understood by ordinary computer users, it will also prove useful for experienced IT users aiming to understand the ins and outs of ransomware threats without diving deep into the technical jargon of the internal structure of ransomware.

mimecast awareness training actors: Cloud Computing Venkata Josyula, Malcolm Orr, Greg Page, 2012 The complete guide to provisioning and managing cloud-based Infrastructure as a Service (IaaS) data center solutions Cloud computing will revolutionize the way IT resources are deployed, configured, and managed for years to come. Service providers and customers each stand to realize tremendous value from this paradigm shift--if they can take advantage of it. Cloud Computing brings together the realistic, start-to-finish guidance they need to plan, implement, and manage cloud solution architectures for tomorrow's virtualized data centers. It introduces cloud newcomers to essential concepts, and offers experienced operations professionals detailed guidance on delivering Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a

Service (SaaS). This book's replicable solutions and fully-tested best practices will help enterprises, service providers, consultants, and Cisco partners meet the challenge of provisioning end-to-end cloud infrastructures. Drawing on extensive experience working with leading cloud vendors and integrators, the authors present detailed operations workflow examples, proven techniques for operating cloud-based network, compute, and storage infrastructure; a comprehensive management reference architecture; and a complete case study demonstrating rapid, lower-cost solutions design. Cloud Computing will be an indispensable resource for all network/IT professionals and managers involved with planning, implementing, or managing the next generation of cloud computing services. Venkata (Josh) Josyula, Ph.D., CCIE(R) No. 13518 is a Distinguished Services Engineer in Cisco Services Technology Group (CSTG) and advises Cisco customers on OSS/BSS architecture and solutions. Malcolm Orr, Solutions Architect for Cisco's Services Technology Solutions, advises telecoms and enterprise clients on architecting, building, and operating OSS/BSS and cloud management stacks. He is Cisco's lead architect for several Tier 1 public cloud projects. Greg Page has spent the last eleven years with Cisco in technical consulting roles relating to data center architecture/technology and service provider security. He is now exclusively focused on developing cloud/IaaS solutions with service providers and systems integrator partners. - Review the key concepts needed to successfully deploy clouds and cloud-based services - Transition common enterprise design patterns and use cases to the cloud - Master architectural principles and infrastructure designs for real-time managed IT services - Understand the Cisco approach to cloud-related technologies, systems, and services - Develop a cloud management architecture using ITIL, TMF, and ITU-TMN standards - Implement best practices for cloud service provisioning, activation, and management - Automate cloud infrastructure to simplify service delivery, monitoring, and assurance - Choose and implement the right billing/chargeback approaches for your business - Design and build IaaS services, from start to finish - Manage the unique capacity challenges associated with sporadic, real-time demand - Provide a consistent and optimal cloud user experience This book is part of the Networking Technology Series from Cisco Press(R), which offers networking professionals valuable information for constructing efficient networks, understanding new technologies, and building successful careers. Category: Cloud Computing Covers: Virtualized Data Centers

mimecast awareness training actors: Broken Trust Trey Herr, Will Loomis, Emma Schroeder, Stewart Scott, Simon Handler, Tianjiu Zuo, 2021-03-29

mimecast awareness training actors: Imagining the Internet Janna Quitney Anderson, 2005-07-21 In the early 1990s, people predicted the death of privacy, an end to the current concept of 'property,' a paperless society, 500 channels of high-definition interactive television, world peace, and the extinction of the human race after a takeover engineered by intelligent machines. Imagining the Internet zeroes in on predictions about the Internet's future and revisits past predictions—and how they turned out. It gives the history of communications in a nutshell, illustrating the serious impact of pervasive networks and how they will change our lives over the next century.

mimecast awareness training actors: Targeted Cyber Attacks Aditya Sood, Richard Enbody, 2014-04-18 Cyber-crime increasingly impacts both the online and offline world, and targeted attacks play a significant role in disrupting services in both. Targeted attacks are those that are aimed at a particular individual, group, or type of site or service. Unlike worms and viruses that usually attack indiscriminately, targeted attacks involve intelligence-gathering and planning to a degree that drastically changes its profile. Individuals, corporations, and even governments are facing new threats from targeted attacks. Targeted Cyber Attacks examines real-world examples of directed attacks and provides insight into what techniques and resources are used to stage these attacks so that you can counter them more effectively. - A well-structured introduction into the world of targeted cyber-attacks - Includes analysis of real-world attacks - Written by cyber-security researchers and experts

mimecast awareness training actors: Adoption and impact of OER in the Global South Hodgkinson-Williams, Cheryl, Arinto, Patricia Brazil, 2018-01-05 Education in the Global South faces

several key interrelated challenges, for which Open Educational Resources (OER) are seen to be part of the solution. These challenges include: unequal access to education; variable quality of educational resources, teaching, and student performance; and increasing cost and concern about the sustainability of education. The Research on Open Educational Resources for Development (ROER4D) project seeks to build on and contribute to the body of research on how OER can help to improve access, enhance quality and reduce the cost of education in the Global South. This volume examines aspects of educator and student adoption of OER and engagement in Open Educational Practices (OEP) in secondary and tertiary education as well as teacher professional development in 21 countries in South America, Sub-Saharan Africa and South and Southeast Asia. The ROER4D studies and syntheses presented here aim to help inform Open Education advocacy, policy, practice and research in developing countries.

mimecast awareness training actors: Narrative Design Michael Breault, 2020-04-22 Narrative designers and game designers are critical to the development of digital and analog games. This book provides a detailed look at the work writers and designers perform every day on game development projects. It includes practical advice on how to break into the game industry as a writer or game designer. Readers can use the templates and detailed instructions provided here to create lively portfolios that will help open the door to jobs in the game industry. Key features of this book: • An intimate look at the workings of AAA game development from someone who has spent decades embedded on teams at well-known companies. • An insider's look at the game industry, including advice on breaking into the industry. • Detailed instructions for creating a portfolio to demonstrate narrative design and game design skills to prospective employers. • Lessons and exercises to help students develop narrative design and game design skills. • A how-to guide for college instructors teaching classes in narrative design and game design. Detailed assignments and syllabi are included. Author Bio: Michael Breault is a 35-year industry veteran who has contributed his writing and game design skills to over 130 published games. He currently teaches narrative design and game design courses at Webster University in St. Louis. The courses he creates and teaches are based on the tasks narrative designers and game designers undertake every day while developing games. These classes provide his students with a real-world view of the work they will be doing as writers and designers in the game industry.

mimecast awareness training actors: *Intelligence-Driven Incident Response* Scott J Roberts, Rebekah Brown, 2017-08-21 Using a well-conceived incident response plan in the aftermath of an online security breach enables your team to identify attackers and learn how they operate. But, only when you approach incident response with a cyber threat intelligence mindset will you truly understand the value of that information. With this practical guide, you'll learn the fundamentals of intelligence analysis, as well as the best ways to incorporate these techniques into your incident response process. Each method reinforces the other: threat intelligence supports and augments incident response, while incident response generates useful threat intelligence. This book helps incident managers, malware analysts, reverse engineers, digital forensics specialists, and intelligence analysts understand, implement, and benefit from this relationship. In three parts, this in-depth book includes: The fundamentals: get an introduction to cyber threat intelligence, the intelligence process, the incident-response process, and how they all work together Practical application: walk through the intelligence-driven incident response (IDIR) process using the F3EAD process—Find, Fix Finish, Exploit, Analyze, and Disseminate The way forward: explore big-picture aspects of IDIR that go beyond individual incident-response investigations, including intelligence team building

mimecast awareness training actors: 7 Rules to Influence Behaviour and Win at Cyber Security Awareness Chirag D Joshi, 2019-07-17 Cyber Security explained in non-cyber language. Get ready to have everything you thought you knew about Cyber Security Awareness challenged. Fight back against the scourge of scams, data breaches, and cyber crime by addressing the human factor. Using humour, real-world anecdotes, and experiences, this book introduces seven simple rules to communicate cyber security concepts effectively and get the most value from your cyber awareness

initiatives. Since one of the rules is Don't Be Boring, this proven process is presented in an entertaining manner without relying on scary numbers, boring hoodie-wearing hacker pictures, or techie jargon! Additionally, this book addresses the What and Why of cyber security awareness in layman's terms, homing in on the fundamental objective of cyber awareness-how to influence user behaviour and get people to integrate secure practices into their daily lives.It draws wisdom from several global bodies of knowledge in the technology domain and incorporates relevant teachings from outside the traditional cyber areas, such as behavioural psychology, neuroscience, and public health campaigns. This book is for everyone, regardless of their prior cyber security experience. This includes cyber security and IT professionals, change managers, consultants, communication specialists, senior executives, as well as those new to the world of cyber security. What Will This Book Do for You? If you're new to cyber security, it will help you understand and communicate the topic better. It will also give you a clear, jargon-free action plan and resources to jump start your own security awareness efforts. If you're an experienced cyber security professional, it will challenge your existing assumptions and provide a better way to increase the effectiveness of your cyber awareness programs. It will empower you to influence user behaviour and subsequently reduce cyber incidents caused by the human factor. It will enable you to avoid common mistakes that make cyber security awareness programs ineffective. It will help make you a more engaging leader and presenter. Most importantly, it won't waste your time with boring content (yes, that's one of the rules!). About the Author Chirag's ambitious goal is simple-to enable human progress through technology. To accomplish this, he wants to help build a world where there is trust in digital systems, protection against cyber threats, and a safe environment online for communication, commerce, and engagement. He is especially passionate about the safety of children and vulnerable sections of society online. This goal has served as a motivation that has led Chirag to become a sought-after speaker and advocate at various industry-leading conferences and events across multiple countries. Chirag has extensive experience working directly with the C-suite executives to implement cyber security awareness training programs. During the course of his career spanning over a decade across multiple sectors, he has built, implemented, and successfully managed cyber security, risk management, and compliance programs. As a leader holding senior positions in organizations, Chirag excels at the art of translating business and technical speak in a manner that optimizes value. Chirag has also conducted several successful cyber training and awareness sessions for non-technical audiences in diverse industries such as finance, energy, healthcare, and higher education. Chirag's academic qualifications include a master's degree in telecommunications management and a bachelor's degree in electronics and telecommunications. He holds multiple certifications, including Certified Information Security Manager, Certified Information Systems Auditor, and Certified in Risk and Information Systems Control.

mimecast awareness training actors: CompTIA Advanced Security Practitioner (CASP) CAS-003 Cert Guide Robin Abernathy, Troy McMillan, 2018-05-11 This is the eBook version of the print title. Note that the eBook may not provide access to the practice test software that accompanies the print book. Learn, prepare, and practice for CompTIA Advanced Security Practitioner (CASP) CAS-003 exam success with this CompTIA Approved Cert Guide from Pearson IT Certification, a leader in IT Certification learning and a CompTIA Authorized Platinum Partner. Master CompTIA Advanced Security Practitioner (CASP) CAS-003 exam topics Assess your knowledge with chapter-ending quizzes Review key concepts with exam preparation tasks CompTIA Advanced Security Practitioner (CASP) CAS-003 Cert Guide is a best-of-breed exam study guide. Leading security certification training experts Robin Abernathy and Troy McMillan share preparation hints and test-taking tips, helping you identify areas of weakness and improve both your conceptual knowledge and hands-on skills. Material is presented in a concise manner, focusing on increasing your understanding and retention of exam topics. The book presents you with an organized test preparation routine through the use of proven series elements and techniques. Exam topic lists make referencing easy. Chapter-ending Exam Preparation Tasks help you drill on key concepts you must know thoroughly. Review questions help you assess your knowledge, and a final

preparation chapter guides you through tools and resources to help you craft your final study plan. Well-regarded for its level of detail, assessment features, and challenging review questions and exercises, this CompTIA approved study guide helps you master the concepts and techniques that will enable you to succeed on the exam the first time, including: Enterprise security Risk management and incident response Research, analysis, and assessment Integration of computing, communications, and business disciplines Technical integration of enterprise components

mimecast awareness training actors: *Cyberheist* Stu Sjouwerman, 2011

mimecast awareness training actors: Security+ Certification For Dummies Lawrence C. Miller, Peter H. Gregory, 2003-03-07 * Prepares readers for the newest vendor-neutral, industry-sponsored IT security exam, an attractive certification option for system security personnel * Security+ has been endorsed by major players like Microsoft, IBM, and the Department of Defense and is expected to become a prerequisite for many vendor-specific certifications * A fast, easy way for IT professionals to learn what they need to qualify for a security credential that is less expensive and less time-consuming than CISSP, SSCP, or SANS GIAC * Author's experience includes security consulting for multinational concerns and systems security management in the U.S. Navy * CD-ROM includes hundreds of randomly-generated bonus test questions and both timed and untimed versions of the practice test

mimecast awareness training actors: Beyond Data Protection Noriswadi Ismail, Edwin Lee Yong Cieh, 2013-02-26 The book deals with data protection issues from practical viewpoints. 40% of the content focus on the Malaysian Personal Data Protection Act (PDPA) 2010 progress, whilst 60% of the content focus on leading comparative practical guidance from Europe. Part of the PDPA provisions is mirrored from European approaches and practices. The approach of this book is straightforward, handy and readable and is supplemented by practical applications, illustrations, tables and diagrams. Practical examples highlighted in this book range from cloud computing, radio frequency identification technology, social media networks and information security to basic related aspects of data protection issues covering strategic leadership, management, governance and audit in businesses, organisations and local authorities. Recommended best practices have been outlined for practical guidance accompanied with future challenges and opportunities for Malaysia and ASEAN. The book is equally suitable for academics, practitioners, governmental officials and regulators dealing with data protection within their sector-specific legislation.

mimecast awareness training actors: Inside Jobs Joe Payne, Jadee Hanson, Mark Wojtasiak, 2020-09-29 From data security company Code42, Inside Jobs offers companies of all sizes a new way to secure today’s collaborative cultures—one that works without compromising sensitive company data or slowing business down. Authors Joe Payne, Jadee Hanson, and Mark Wojtasiak, seasoned veterans in the cybersecurity space, provide a top-down and bottom-up picture of the rewards and perils involved in running and securing organizations focused on rapid, iterative, and collaborative innovation. Modern day data security can no longer be accomplished by “Big Brother” forms of monitoring or traditional prevention solutions that rely solely on classification and blocking systems. These technologies frustrate employees, impede collaboration, and force productivity work-arounds that risk the very data you need to secure. They provide the illusion that your trade secrets, customer lists, patents, and other intellectual property are protected. That couldn’t be farther from the truth, as insider threats continue to grow. These include: Well-intentioned employees inadvertently sharing proprietary data Departing employees taking your trade secrets with them to the competition A high-risk employee moving source code to an unsanctioned cloud service What’s the solution? It’s not the hunt for hooded, malicious wrongdoers that you might expect. The new world of data security is built on security acting as an ally versus an adversary. It assumes positive intent, creates organizational transparency, establishes acceptable data use policies, increases security awareness, and provides ongoing training. Whether you are a CEO, CIO, CISO, CHRO, general counsel, or business leader, this book will help you understand the important role you have to play in securing the collaborative cultures of the future.

mimecast awareness training actors: Windows Forensics Philip Polstra, 2016-07-16

Windows Forensics is the most comprehensive and up-to-date resource for those wishing to leverage the power of Linux and free software in order to quickly and efficiently perform forensics on Windows systems. It is also a great asset for anyone that would like to better understand Windows internals. Windows Forensics will guide you step by step through the process of investigating a computer running Windows. Whatever the reason for performing forensics on a Windows system, be it incident response, a criminal investigation, suspected data ex-filtration, or data recovery, this book will tell you what you need to know in order to perform the vast majority of investigations. All of the tools discussed in this book are free and most are also open source. Dr. Philip Polstra shows how to leverage numerous tools such as Python, shell scripting, and MySQL to quickly, easily, and accurately analyze Windows systems. While readers will have a strong grasp of Python and shell scripting by the time they complete this book, no prior knowledge of either of these scripting languages is assumed. Windows Forensics begins by showing you how to determine if there was an incident with minimally invasive techniques. Once it appears likely that an incident has occurred, Dr. Polstra shows you how to collect data from a live system before shutting it down for the creation of filesystem images. Windows Forensics contains extensive coverage of Windows FAT and NTFS filesystems. A large collection of Python and shell scripts for creating, mounting, and analyzing filesystem images are presented in this book. The treasure trove of data found in the Windows Registry and other artifacts are discussed in detail. Dr. Polstra introduces readers to the exciting new field of memory analysis using the Volatility framework. Discussion of malware analysis rounds out the book. Book Highlights 554 pages in large, easy-to-read 8.5 x 11 inch format Over 11,000 lines of Python scripts with explanations Over 500 lines of shell and command scripts with explanations A 96 page chapter covering the FAT filesystem in detail A 164 page chapter on NTFS filesystems Multiple scenarios described in detail with images available from the book website All scripts and other support files are available from the book website

mimecast awareness training actors: Organic Food Systems Raymond Auerbach, 2019 This book reports on long-term comparative organic farming systems' research trials carried out over the last 5 years in the Southern Cape of South Africa, as well as research into the successes and failures of the organic sector and the technical tools required for sustainable development in South Africa, Zambia, Uganda and Tanzania. It includes 24 chapters organized into 4 parts. Part 1 (Chapters 1-6) discusses the historical development of organic farming systems, examines the global issues which confront us, and develops some concepts showing a progression in small-scale farmer development and how this can be supported with appropriate training and policy. The difference between national food self-sufficiency and household food security is examined, and the organic sector is introduced. Part 2 (Chapters 7-14) deals with capacity building and climate change. Holistic systems, inclusive participatory approaches, institution building and experiential learning are examined. Organic food production, farmer training, value chains, impact of drought on food prices and food availability, and urban water and energy use efficiency are described. Part 3 (Chapters 15-22) presents evidence on how to support organic farmers. It starts with 2 case studies on the well-developed organic sector in Uganda and the developing one in Zambia. The following chapters discuss soil carbon determination, comparison of organic and conventional farming systems, pest and disease control (e.g., chemical, holistic and biological control), soil fumigation, soil microbiology in organic and conventional systems, soil fertility changes and crop yield. Part 4 (Chapters 23-24) makes strategic suggestions about how to upscale organic farming and organic food systems in Southern Africa. This book is a vital resource for all stakeholders in organic agriculture.

mimecast awareness training actors: Business Communication Mary Ellen Guffey, Patricia Rogin, Kathleen Rhodes, 2001

mimecast awareness training actors: YoungGiftedandFat Sharrell D. Luckett, 2017-11-15 YoungGiftedandFat is a critical autoethnography of performing thin– on the stage and in life. Sharrell D. Luckett’s story of weight loss and gain and playing the (beautiful, desirable, thin) leading lady showcases an innovative and interdisciplinary approach to issues of weight and self-esteem, performance, race, and gender. Sharrell structures her project with creative text, interviews,

testimony, journal entries, dialogues, monologues, and deep theorizing through and about the abundance of flesh. She explores the politics of Black culture, and particularly the intersections of her lived and embodied experiences. Her body and body transformation becomes a critical praxis to evidence fat as a feminist issue, fat as a Black-girl-woman issue, and fat as an ideological construct that is as much on the brain as it is on the body. YoungGiftedandFat is useful to any area of research or course offering taking up questions of size politics at the intersections of race and sexuality.

mimecast awareness training actors: *Future Crimes* Marc Goodman, 2015-02-24 From one of the world's leading authorities on global security, Future Crimes takes readers deep into the digital underground to illuminate the alarming ways criminals, corporations, and even countries are using new and emerging technologies against you—and how this makes everyone more vulnerable than you ever thought possible. Technological advances have benefited our world in immeasurable ways—but there is an ominous flip side. Criminals are often the earliest, and most innovative, adopters of technology, and modern times have lead to modern crimes. Today's criminals are stealing identities, draining online bank accounts and wiping out computer servers. It's disturbingly easy to activate baby monitors to spy on families, pacemakers can be hacked to deliver a lethal jolt of electricity, and thieves are analyzing your social media in order to determine the best time for a home invasion. Meanwhile, 3D printers produce AK-47s, terrorists can download the recipe for the Ebola virus, and drug cartels are building drones. This is just the beginning of the tsunami of technological threats coming our way. In Future Crimes, Marc Goodman rips opens his database of hundreds of real cases to give us front-row access to these impending perils. Reading like a sci-fi thriller, but based in startling fact, Future Crimes raises tough questions about the expanding role of technology in our lives. Future Crimes is a call to action for better security measures worldwide, but most importantly, it will empower readers to protect themselves against looming technological threats—before it's too late.

mimecast awareness training actors: Hacking Multifactor Authentication Roger A. Grimes, 2020-09-28 Protect your organization from scandalously easy-to-hack MFA security “solutions” Multi-Factor Authentication (MFA) is spreading like wildfire across digital environments. However, hundreds of millions of dollars have been stolen from MFA-protected online accounts. How? Most people who use multifactor authentication (MFA) have been told that it is far less hackable than other types of authentication, or even that it is unhackable. You might be shocked to learn that all MFA solutions are actually easy to hack. That’s right: there is no perfectly safe MFA solution. In fact, most can be hacked at least five different ways. Hacking Multifactor Authentication will show you how MFA works behind the scenes and how poorly linked multi-step authentication steps allows MFA to be hacked and compromised. This book covers over two dozen ways that various MFA solutions can be hacked, including the methods (and defenses) common to all MFA solutions. You’ll learn about the various types of MFA solutions, their strengthens and weaknesses, and how to pick the best, most defensible MFA solution for your (or your customers') needs. Finally, this book reveals a simple method for quickly evaluating your existing MFA solutions. If using or developing a secure MFA solution is important to you, you need this book. Learn how different types of multifactor authentication work behind the scenes See how easy it is to hack MFA security solutions—no matter how secure they seem Identify the strengths and weaknesses in your (or your customers’) existing MFA security and how to mitigate Author Roger Grimes is an internationally known security expert whose work on hacking MFA has generated significant buzz in the security world. Read this book to learn what decisions and preparations your organization needs to take to prevent losses from MFA hacking.

mimecast awareness training actors: The Art and Science of Creativity George Frederick Kneller, 1965

mimecast awareness training actors: *Multimodal Literacy* Carey Jewitt, Gunther R. Kress, 2003 Multimodal Literacy challenges dominant ideas around language, learning, and representation. Using a rich variety of examples, it shows the range of representational and communicational modes involved in learning through image, animated movement, writing, speech, gesture, or gaze. The

effect of these modes on learning is explored in different sites including formal learning across the curriculum in primary, secondary, and higher education classrooms, as well as learning in the home. The notion of literacy and learning as a primary linguistic accomplishment is questioned in favor of the multimodal character of learning and literacy. By illustrating how a range of modes contributes to the shaping of knowledge and what it means to be a learner, Multimodal Literacy provides a multimodal framework and conceptual tools for a fundamental rethinking of literacy and learning.

mimecast awareness training actors: Alice and Bob Learn Application Security Tanya Janca, 2020-11-10 Learn application security from the very start, with this comprehensive and approachable guide! Alice and Bob Learn Application Security is an accessible and thorough resource for anyone seeking to incorporate, from the beginning of the System Development Life Cycle, best security practices in software development. This book covers all the basic subjects such as threat modeling and security testing, but also dives deep into more complex and advanced topics for securing modern software systems and architectures. Throughout, the book offers analogies, stories of the characters Alice and Bob, real-life examples, technical explanations and diagrams to ensure maximum clarity of the many abstract and complicated subjects. Topics include: Secure requirements, design, coding, and deployment Security Testing (all forms) Common Pitfalls Application Security Programs Securing Modern Applications Software Developer Security Hygiene Alice and Bob Learn Application Security is perfect for aspiring application security engineers and practicing software developers, as well as software project managers, penetration testers, and chief information security officers who seek to build or improve their application security programs. Alice and Bob Learn Application Security illustrates all the included concepts with easy-to-understand examples and concrete practical applications, furthering the reader's ability to grasp and retain the foundational and advanced topics contained within.

mimecast awareness training actors: *Healthcare Cybersecurity* W. Andrew H. Gantt, III, 2021-09-07 This book pinpoints current and impending threats to the healthcare industry's data security.

mimecast awareness training actors: Hacked Again Scott N. Schober, 2016-03-15 Hacked Again details the ins and outs of cybersecurity expert and CEO of a top wireless security tech firm Scott Schober, as he struggles to understand: the motives and mayhem behind his being hacked. As a small business owner, family man and tech pundit, Scott finds himself leading a compromised life. By day, he runs a successful security company and reports on the latest cyber breaches in the hopes of offering solace and security tips to millions of viewers. But by night, Scott begins to realize his worst fears are only a hack away as he falls prey to an invisible enemy. When a mysterious hacker begins to steal thousands from his bank account, go through his trash and rake over his social media identity; Scott stands to lose everything he worked so hard for. But his precarious situation only fortifies Scott's position as a cybersecurity expert and also as a harbinger for the fragile security we all cherish in this digital life. Amidst the backdrop of major breaches such as Target and Sony, Scott shares tips and best practices for all consumers concerning email scams, password protection and social media overload: Most importantly, Scott shares his own story of being hacked repeatedly and bow he has come to realize that the only thing as important as his own cybersecurity is that of his readers and viewers. Part cautionary tale and part cyber self-help guide, Hacked Again probes deep into the dark web for truths and surfaces to offer best practices and share stories from an expert who has lived as both an enforcer and a victim in the world of cybersecurity. Book jacket.

mimecast awareness training actors: *The Incident Response System* , 1986

mimecast awareness training actors: Phishing Dark Waters Christopher Hadnagy, Michele Fincher, 2015-04-06 An essential anti-phishing desk reference for anyone with an email address Phishing Dark Waters addresses the growing and continuing scourge of phishing emails, and provides actionable defensive techniques and tools to help you steer clear of malicious emails. Phishing is analyzed from the viewpoint of human decision-making and the impact of deliberate influence and manipulation on the recipient. With expert guidance, this book provides insight into the financial, corporate espionage, nation state, and identity theft goals of the attackers, and teaches

you how to spot a spoofed e-mail or cloned website. Included are detailed examples of high profile breaches at Target, RSA, Coca Cola, and the AP, as well as an examination of sample scams including the Nigerian 419, financial themes, and post high-profile event attacks. Learn how to protect yourself and your organization using anti-phishing tools, and how to create your own phish to use as part of a security awareness program. Phishing is a social engineering technique through email that deceives users into taking an action that is not in their best interest, but usually with the goal of disclosing information or installing malware on the victim's computer. Phishing Dark Waters explains the phishing process and techniques, and the defenses available to keep scammers at bay. Learn what a phish is, and the deceptive ways they've been used Understand decision-making, and the sneaky ways phishers reel you in Recognize different types of phish, and know what to do when you catch one Use phishing as part of your security awareness program for heightened protection Attempts to deal with the growing number of phishing incidents include legislation, user training, public awareness, and technical security, but phishing still exploits the natural way humans respond to certain situations. Phishing Dark Waters is an indispensible guide to recognizing and blocking the phish, keeping you, your organization, and your finances safe.

mimecast awareness training actors: USB Forensics Philip Polstra, 2017-07-06

mimecast awareness training actors: Cyber Insecurity Richard Harrison, Trey Herr, 2016-10-18 Growing dependence on cyberspace for commerce, communication, governance, and military operations has left society vulnerable to a multitude of security threats. Mitigating the inherent risks associated with the use of cyberspace poses a series of thorny public policy problems. In this volume, academics, practitioners from both private sector and government, along with former service members come together to highlight sixteen of the most pressing contemporary challenges in cybersecurity, and to offer recommendations for the future. As internet connectivity continues to spread, this book will offer readers greater awareness of the threats of tomorrow—and serve to inform public debate into the next information age. Contributions by Adrienne Allen, Aaron Brantly, Lauren Boas Hayes, Jane Chong, Joshua Corman, Honorable Richard J. Danzig, Kat Dransfield, Ryan Ellis, Mailyn Fidler, Allan Friedman, Taylor Grossman, Richard M. Harrison, Trey Herr, Drew Herrick, Jonah F. Hill, Robert M. Lee, Herbert S. Lin, Anastasia Mark, Robert Morgus, Paul Ohm, Eric Ormes, Jason Rivera, Sasha Romanosky, Paul Rosenzweig, Matthew Russell, Nathaniel Tisa, Abraham Wagner, Rand Waltzman, David Weinstein, Heather West, and Beau Woods.

mimecast awareness training actors: Managed Code Rootkits Erez Metula, 2010-11-25 Managed Code Rootkits is the first book to cover application-level rootkits and other types of malware inside the application VM, which runs a platform-independent programming environment for processes. The book, divided into four parts, points out high-level attacks, which are developed in intermediate language. The initial part of the book offers an overview of managed code rootkits. It explores environment models of managed code and the relationship of managed code to rootkits by studying how they use application VMs. It also discusses attackers of managed code rootkits and various attack scenarios. The second part of the book covers the development of managed code rootkits, starting with the tools used in producing managed code rootkits through their deployment. The next part focuses on countermeasures that can possibly be used against managed code rootkits, including technical solutions, prevention, detection, and response tactics. The book concludes by presenting techniques that are somehow similar to managed code rootkits, which can be used in solving problems. - Named a 2011 Best Hacking and Pen Testing Book by InfoSec Reviews - Introduces the reader briefly to managed code environments and rootkits in general - Completely details a new type of rootkit hiding in the application level and demonstrates how a hacker can change language runtime implementation - Focuses on managed code including Java, .NET, Android Dalvik and reviews malware development scanarios

mimecast awareness training actors: Urban Planning for Disaster Recovery Alan March, Maria Kornakova, 2017-05-10 Urban Planning for Disaster Recovery focuses on disaster recovery from the perspective of urban planning, an underutilized tactic that can significantly reduce disaster risks. The book examines disaster risk reduction (DRR), in particular, the recovery stage of what is

widely known as the disaster cycle. The theoretical underpinning of the book derives from a number of sources in urban planning and disaster management literature, and is illustrated by a series of case studies. It consists of five sections, each of which opens with a conceptual framework that is followed by a series of supporting and illustrative cases as practical examples. These examples both complement and critique the theoretical base provided, demonstrating the need to apply the concepts in location-specific ways. - Examines disaster recovery from an urban planning perspective - Illustrates key concepts with real-world case studies - Explores the contributions of experts, urban planners, NGOs, and community members

mimecast awareness training actors: Can I See your Hands Gavriel Schneider, 2017-09-01 The title of this book: CAN I SEE YOUR HANDS refers to one of the key outcomes of this book--being able to tell whether or not people want to cause us harm. To put it very simply, if you can see someone's hands and they are not concealing them, holding a weapon or positioning to strike you, one's levels of trust and confidence can increase. This simple example can serve as a reminder to all of us in many of the complex moments we have to deal with, and difficult decisions we have to make, in everyday life.