LAI Leading Authorities, Inc.

Jenny Radcliffe

People Hacker and Social Engineer

Only Human: Social Engineering and People Hacking in a Cyber Age. In this talk “People Hacker” Jenny Radcliffe discusses the ongoing and persistent threat of Social Engineering, or human-based attacks, on businesses of all types and sizes. The talk covers how the cultural and human elements of an organization can help inform and shape the nature of these attacks and how glitches in our own thinking can be exploited to facilitate the cons, scams and attacks used by malicious social engineers. Jenny will talk about her own experiences as an ethical Social Engineer and will discuss the tricks, tactics and methods she uses to attack organisations via their people. She will give tips and guidance on how to “wake up the workforce” to the threat of Social Engineering, and will discuss how to maintain the engagement of all staff to help you prevent these attackers from targeting your organization through its people.

The Human Element of Security: How to Become a People Hacker. From an early age, locked doors, high fences, and the secrets kept by businesses, buildings and people, fascinated Jenny Radcliffe. She has spent a lifetime learning how to use the “human element” to gain access to the buildings, data and information. This talk is an anecdote-ridden roller coaster of a tale which takes the audience from the mean streets of Liverpool in the 1980’s to the square mile of London’s financial district and beyond. Jenny shares her journey from breaching zoos, offices, theme parks, banks and football matches, to helping respected businesses and organisations protect themselves from the threat of malicious “people hackers.” Expect to takeaway high-ROI insights on reading social cues, protecting against exploitation, lie detection and negotiation techniques, and thinking about social intelligence in an entirely new way.

The Perfect Storm: How Culture, Coincidences, and Con Artists Social Engineer Past Your Security. Jenny Radcliffe a.k.a “The People Hacker” has been getting past security systems using non-technical methods all her life. In this energetic and informative talk she will discuss why the “human element” is still such a popular way to “hack” into organisations, and why it is so difficult to “patch” this area of a company. The talk discusses how an organization can be “profiled” by a malicious human hacker, who then uses this information to design a hack that will work well within the culture of the target company. She will explain why culture is such an important element in the shape and nature of an attack on an organization, as well as in communicating the threat to its people and ultimately in the defense against attacks. Jenny will talk about her own experiences as an ethical Social Engineer and will discuss the tricks, tactics and methods she uses to attack organisations via their people. She will give tips and guidance on how to “wake up the workforce” to the threat of Social Engineering, and will discuss how to maintain the engagement of all staff to help you prevent these threats from hitting your organization through its people.

Social Engineering, Culture and Coincidence: Why and How your "People Hacks" are Getting Personal and What You Can do to Stop Them. Social engineering attacks continue to present a huge threat to organisations of all sizes, as increasingly sophisticated technology makes targeting the human element an easier way "in" for a hacker. But why are some companies easier to target than others? What makes the people element of organisations so vulnerable and more particularly how is your company culture likely to shape the more targeted and sophisticated attacks upon your own organisation. In this talk Jenny Radcliffe a.k.a "The People Hacker" links organizational culture and personality to the methodology of malicious Social Engineers. She explains how a company profile "invites" a tailored hack and what might be done to prevent it. She explains the importance of "waking up the workforce" to the threat and suggests how to do so effectively, using the same psychological methods the hackers might be deploying to try catch them out!

Adventures in Social Engineering…. Tales of a "People Hacker." ***How Jenny Radcliffe spend her life getting past security, stealing the show, and smiling her way into banks, businesses, buildings and the tower of London through "hacking" the people!*** From an early age, locked doors, high fences and the secrets kept by businesses, buildings and people, fascinated Jenny Radcliffe. She has spent a lifetime learning how to use the "human element" to gain access to the buildings, data and information. A burgular for hire, a con-artist and an expert in Non-verbal communications, deception and persuasion techniques, she is an ethical Social Engineer, a "people hacker" hired to smash security measures, using psychology, stage craft, illusion and subliminal linguistics rather than technical hacking techniques. The aim of these activities to is educate and train the workforce from the boardroom to the front desk, in how to prevent similar attacks from malicious individuals. Jenny shows businesses how to mitigate themselves from being conned and scammed by those who would use these techniques to cause real disruption and harm. This talk is an anecdote ridden roller coaster of a tale which takes the audience from the mean streets of Liverpool in the 1980's to the square mile of London's financial district and beyond. Of hiding under desks and climbing walls, of picking locks and dumpster diving, of acting skills and quick thinking and of living to tell the tale. It tells of Jenny's journey from breaching zoos, offices and funeral parlours, theme parks, banks and football matches, to helping respected businesses and organisations to protect themselves from the threat of malicious "people hackers." Learn how, without technology, Jenny uses the "machine between our ears" to "psychologically pen-test" companies, find the weaknesses in their security measures, and help bolster their human defenses against future attacks.

Sleepless in Security: Waking Up Your workforce to the Threat of Social Engineering. Many organisations do not give Social Engineering the time and attention it warrants as part of their security strategy. Non-technical "hacks" targeting people and manipulating them into giving access to information, data and physical locations can be just as devastating as a more technical attack, but awareness of the threat and its consequences remains low in many companies. When the human element of an organization is manipulated, coerced and conned into assisting an attacker the consequences can be felt not only in financial terms but also in the cultural and psychological damage that follows. Yet, there is often very little time and energy spent on the problem in terms of

creating awareness and increasing defenses against such attacks, in many companies. People are often unaware of the shape and nature of attacks and are almost “asleep” when it comes to defending themselves, and their companies, against this type of threat. In this talk, Jenny Radcliffe a.k.a “The People Hacker” will discuss the many ways a social engineer might target your workforce. The methods used to persuade them to give up valuable details that should be kept private, and the manner in which Social Engineering can form part of a wider, more technical attack. She gives advice on communicating the dangers of Social Engineering to the workforce, and discusses how to hold their attention and “wake” people up to the risks we all face from these determined and skillful “human” attackers.

Motivations, Misdirection and Mal-intent: The Evolving Dark Psychology of the New Social Engineers. Social Engineering remains a little understood area of security, and yet understanding the “human element” of security, and protecting our people from manipulation by malicious Social Engineers , is an essential element of compliance. In this talk, Jenny Radcliffe describes how damaging Social Engineering attacks might be, how the culture of your organization may help “shape and invite” a Social Engineering attack, and how you need to work within your existing cultural norms to protect your organization against future threats. Understand the motivations and methodology behind Social Engineering Link organizational culture with different types of Social Engineering attacks Learn how to use your own cultural footprint as a defense against Social Engineers

The Evolution of the Con: Understanding and Avoiding Modern-Day Scams, Cons, and Fraud. Con-artists have been around throughout history from Trojan Horses to Snake Oil, Ponzi Schemes to double agents, and much of the fundamental psychology used to exploit victims has barely changed. However, modern technology has allowed criminals to scam individuals and businesses on a faster and wider scale than ever before. So, if we understand how con-artists work, why is it that many businesses and individuals still fall for the modern-day equivalent of the classic con? From phishing emails to romance scams, from social engineering to finance fraud, in this talk professional social engineer and ethical con-artist, Jenny Radcliffe explains how cons, scams, and frauds are constructed. It explores what lessons can be learnt from the hustles and schemes of the past, and how we can all recognise the warning signs to avoid becoming victims of the modern-day criminal con-artist. This talk explores the psychology of human nature and how it can be exploited to lure people into becoming victims. It covers the nature of fear, uncertainty and doubt, how technology has allowed the con to adapt, and why times of turbulence and change provide the perfect environment for criminals to profit from human weakness. The talk provides workable, practical advice on how to protect ourselves from falling for scams, hustles and fraud, and gives workable strategies on how to mitigate and counter the methods used by criminals to exploit both corporate and individual targets. With over 80% of cyber crimes caused by the direct manipulation or exploitation of staff, and with the costs, both financial and human, of falling prey to the criminals rising at an alarming rate, this talk helps to strengthen your defences and create awareness amongst your team of what a scam looks like and how to prevent it.