LAI Leading Authorities, Inc.

Graham Cluley

Award-Winning Tech Security Analyst

30 YEARS OF CYBERCRIME IN 30 MINUTES...

From back bedrooms to boardrooms, Graham Cluley describes how cybercrime turned from a schoolboy prank into a threat able to steal secrets from governments, disrupt Iranian nuclear facilities, and even help secret agents assassinate their opponents. Graham draws on his 30-year history within the industry to explain who the malware authors are, how the nature of the attacks are changing, and the steps companies need to take to prevent themselves becoming the next victims.

STEALING THE CROWN JEWELS

In 1671, Colonel Thomas Blood broke into what should have been the safest place on Earth - the Tower of London - and managed to steal the Crown Jewels.

Today it sounds like an adventure story, but there are lessons that all organisations can learn from this, and other heists which have happened over the centuries, when it comes to protecting their data from malicious hackers.

UNBELIEVABLE STORIES OF CYBERHORROR

Graham Cluley explores some of the surprising and unusual ways that companies have been hacked, and the craziest things tech companies have done to put our data at risk. Learn about the company that claimed it had been hacked but hadn't... all for publicity! (And boy, they got it...)

IT'S TIME TO TAKE PASSWORDS F+++ING SERIOUSLY

Computer security veteran Graham Cluley shares stories of how companies have found themselves in hot water because of security failures, and how stronger authentication and enterprise password management might have helped them secure themselves better.

BUSINESS AS USUAL: HOW CYBERCRIME IS BOOMING DURING THE PANDEMIC

Computer security veteran Graham Cluley describes the biggest threats facing business today, and how cybercriminals are exploiting the Coronavirus crisis, taking advantage of the disruption to steal information from organisations, compromise networks, scam the unwary, and even endangering lives.

LOCKDOWN: HOW CYBERCRIMINALS ARE EXPLOITING THE CORONAVIRUS PANDEMIC

The COVID-19 pandemic has forced hundreds of millions of people to stay in their homes, and businesses have been massively disrupted. As people around the world resort to connecting to the internet from home to work, opportunities for accounts to be hacked and data to be stolen have rocketed. Computer security veteran Graham Cluley describes how cybercriminals are exploiting the Coronavirus crisis to steal information from businesses, compromise networks, scam the unwary, and even launch ransomware attacks against hospitals and the World Health Organisation.

Speaking points:

* The different types of attacks orchestrated by hackers during the pandemic

* Can video conferencing systems be trusted? What security and privacy flaws have been found in the likes of Zoom, and how have political leaders played fast-and-loose with their own security and privacy since lockdown?

* The challenges faced by businesses trying to secure their remote workforce as the lockdown persists...

NOT ALL CYBERCRIMINALS ARE EVIL GENIUSES

The media loves to present hackers as evil geniuses, but that's often not the case. They may not be smart, and they may not be bad. Sometimes they may even be neither! The truth is that good people sometimes do bad

things. And bad people sometimes do very dumb things. Computer security veteran Graham Cluley will take you on a journey through some of dumb mistakes that malicious hackers have made which made it easy for them to be identified - the goofs, the screw-ups, and the basic failings which led to the authorities knocking on their door.

Takeaway bullets:

* Learn from the mistakes of cybercriminals to help protect yourself online

* Understand some of the bizarre motivations that have resulted in crimes being committed on

* Discover how to better defend your company from attacks by having a better understanding of the motivations of hackers.

* Take away tales that you can use to help raise awareness of cyber threats inside your organisation.

HOW TO MAKE A BILLION DOLLARS THROUGH CYBERCRIME

A sophisticated cybercrime gang is responsible for stealing over one billion dollars from banks and financial institutions around the world, targeting individuals involved in SEC filings.

How did they do it? Who are the people behind the gang? And what can be done to protect against this and other attacks by sophisticated organised hacking gangs?

Computer security expert Graham Cluley offers practical insight on how financial firms are being targeted, and shines some light on mysterious and elusive global crime rings.

UNBELIEVABLE STORIES OF CYBER HORROR

Every day we read headlines of data breaches, hacks, and malware attacks. Often they're identikit newspaper stories where you could easily just change the names of the companies involved and the number of customer records they have had stolen from them.

But every now and then something extraordinary happens. Like the companies who pretended to be hacked when they hadn't, or the attackers who went to extraordinary lengths to steal millions from their employers.

In this presentation, computer security veteran Graham Cluley shares some unbelievable tales of cyber attack.

* How hacked companies exploit the media to boost their brand

* How to cheat at the lottery and win $14.3 million

* Recognising the insider threat

* You won't survive unless you're skeptical

Graham Cluley explores some of the surprising and unusual ways that companies have been hacked, and the craziest things tech companies have done to put our data at risk.

THREE THREATS THAT SHOULD BE KEEPING YOU AWAKE AT NIGHT

If you're losing sleep over state-sponsored attackers you're approaching things the wrong way. Yes, intelligence agencies are hacking some firms, but chances are that they're not interested in yours.

Financially-motivated hacks and frauds are on the rise because it has become so easy for attackers to steal large amounts of money. And there's no need for criminals to know how to write malware to potentially steal millions from your business.

Graham Cluley describes the ways businesses are losing data and allowing fraudsters to steal sometimes vast amounts of money, and what you can do to reduce the chances of your firm being the next victim.

TARGETED ATTACKS

The glory days of mass-mailed malware, tricking users into believing they were opening a love letter or a photograph of Anna Kournikova are behind us. Today your company is at risk of being hit by carefully-crafted targeted attack, designed with your business in mind to maximise its potential for success.

Drawing upon examples like Sony, TalkTalk and Ashley Madison Graham Cluley describes the damage that can be done to corporations - not just through the theft of customer data and intellectual property, but also to a company's brand image.

Looking to the future, Graham Cluley discusses how all companies have to be aware that they are potentially fighting a new enemy online - the state-sponsored attacker....

THE RISE OF MALWARE

From back bedrooms to boardrooms, Graham Cluley describes how viruses and trojan horses turned from a schoolboy prank into a threat which could steal secrets from governments, disrupt nuclear facilities in Iran, and even help secret agents assassinate their opponents.

Graham Cluley draws on his long history in the anti-virus industry to explain who the malware authors are, how the nature of the attacks are changing, and the steps that organisations need to take to prevent themselves from becoming the next victim.

THE INTERNET OF INSECURE THINGS

More and more household items are being connected to the internet, often with little thought regarding security. If not taken seriously, the threat could even be deadly.

In the last few months, we have all read headlines of how Jeeps have been remotely hacked while driving at 70mph down the motorway, giving attackers the potential ability to kill the brakes, or interfere with the steering. Meanwhile millions of vehicles have been recalled because vehicles are becoming the ultimate mobile device - computers that we sit in.

We wouldn't dream of attaching a desktop computer to the internet without having security in place, so how come everything from internet-connected toothbrushes to smartphone-controlled washing machines and remote control thermostats are fine to plug in?

The truth is that "smart" devices have the potential to be very very dumb when it comes to security. Unlike PC and software vendors who have decades of computer security experience, the manufacturers of these new devices often have little in the way of expertise and yet could still be exposing us and our personal data to the threat of hackers.

Graham Cluley describes the threat, and calls upon the manufacturers and developers to take the security of these devices more seriously.
