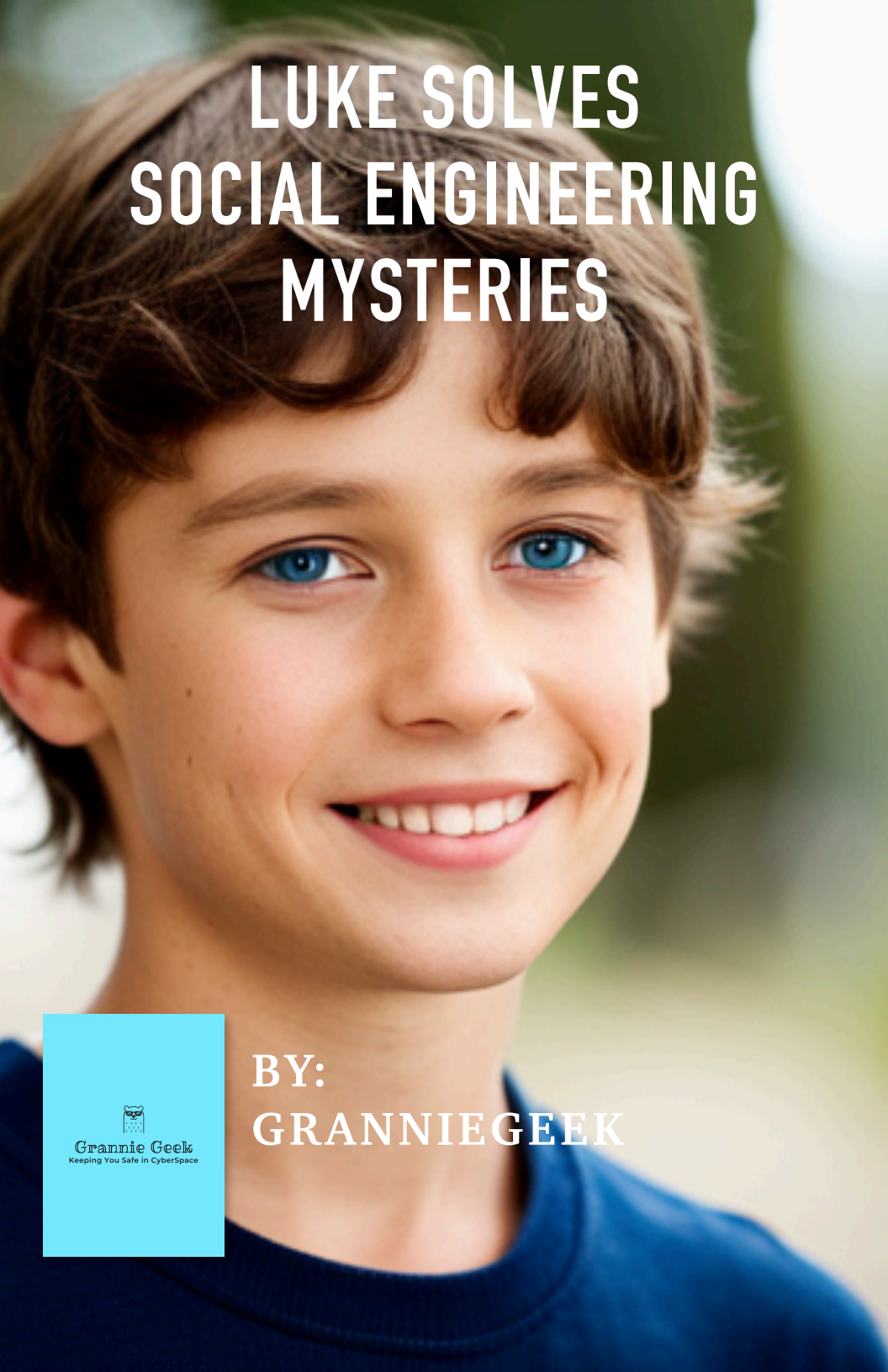
LUKE SOLVES SOCIAL ENGINEERING MYSTERIES



Grannie Geek
Keeping You Safe in CyberSpace

BY:
GRANNIEGEEK

INTRODUCTION

Welcome to the story of Luke, a 12-year-old boy who uses his social engineering skills to solve mysteries. In today's digital age, social engineering has become a prevalent form of cybercrime. It involves manipulating people into giving out sensitive information or performing actions that may compromise their security.

Luke is not your typical 12-year-old boy. He possesses an extraordinary set of skills that allow him to read people's behavior and use it to his advantage. He is a master of persuasion and can easily gain people's trust, making them reveal their deepest secrets.

Join me on this journey as I follow Luke's adventures in solving social engineering mysteries. Along the way, you will learn about different types of social engineering attacks and how to protect yourself from falling victim to them.

Are you ready to join Luke on his mission?

DEDICATION

This book is dedicated to my loving grandson, Luke. Your inquisitive mind, determination and unwavering courage have been an inspiration to me. You are a shining example of what can be achieved when one sets their mind to it.

In the pages that follow, I hope to capture your vibrant spirit and deep understanding of human nature as you solve social engineering mysteries. As you continue to grow and blossom into a remarkable young man, I know that your contributions to the world will be profound. Thank you for being such an incredible grandson and for always being there to brighten my day.

This book is a tribute to you, Luke. May it serve as a reminder of your accomplishments and the endless potential that lies within you.

With much love and admiration,

Grandma (AKA) GrannieGeek

SOCIAL ENGINEERING

Luke was a 12-year-old boy who lived in a small town in the countryside. He was an intelligent and curious kid, always looking for new adventures to embark on. But little did he know that his curiosity would lead him down a dangerous path.

One day, while browsing the internet, Luke stumbled upon something called "social engineering". Intrigued by the term, he clicked on the link and began reading about it. He learned that social engineering is the art of manipulating people into giving out sensitive information or performing certain actions.

Being just a kid, Luke didn't fully understand the consequences of this practice. To him, it seemed like an interesting challenge to see if he could manipulate people into doing what he wanted.

He started with his classmates at school. With his sweet smile and charming personality, Luke easily convinced his friends to lend him their toys or do favors for him. At first, it was all just harmless fun for Luke, but soon enough he realized that he could use this skill for more devious purposes.

He decided to test his abilities on adults next. One afternoon at the grocery store, as his mom was busy picking out vegetables from one aisle over, Luke approached an employee stocking shelves and asked if they had any free samples available. The employee kindly obliged and gave him some cookies without question.

Feeling confident in himself now, Luke set his sights on bigger targets - local businesses and even strangers walking down the street. And shockingly enough, most of them fell prey to young mastermind's tactics without even realizing what had happened.

But things took a turn when one day; while trying to con someone else into giving him money so he could buy ice cream from an ice-cream truck passing by - which worked flawlessly every other time –the person turned out not be as naïve as everyone else did before!

As luck would have it though another adult saw everything transpire between them, and immediately understood what was happening. They promptly approached Luke's mother with the whole story.

Shocked and horrified, his mother sat him down for a long talk about the dangers of social engineering. She explained how it can be used by malicious people to harm others or steal their personal information.

Feeling guilty and ashamed of his actions, Luke promised to never use social engineering again. He learned a valuable lesson that day - that with great power comes great responsibility. And from then on, he used his intelligence for good instead of manipulating people for his own gain.

Together with his curiosity and determination this began his interest in solving social engineering crimes and making a difference in the world.

Years later, Luke became an ethical hacker using his knowledge of social engineering to help companies protect themselves from cyber attacks. But he always remembered the lessons he learned as a 12-year-old boy experimenting with dangerous tactics- always use your powers for good and never take advantage of others.

PHISHING

It was a beautiful summer day in the small town of Maplewood. The sun was shining, birds were chirping and children were playing outside. Among them was Luke, a curious 12-year-old boy who had a knack for solving mysteries.

Luke lived with his parents in a cozy house on the edge of town. His parents worked long hours at the local factory, leaving Luke to entertain himself during the summer holidays. But he didn't mind, as he loved exploring and unraveling secrets.

One day, while scrolling through his emails, Luke received an urgent message from his friend Josh. It read: "Help! I think my mom's laptop has been hacked!"

Intrigued by this cryptic message, Luke quickly replied asking for more details. Josh explained that his mother had received an email claiming to be from their bank requesting personal information due to security concerns.

Without thinking twice, she clicked on the link provided in the email and entered her login details. However, moments later she realized that it might have been a phishing scam when she noticed several unauthorized transactions on her account.

Being well-versed in technology and cyber safety thanks to his father who worked as an IT specialist, Luke immediately knew what needed to be done.

He asked Josh's mother for all the details about the email and started investigating. He traced back the IP address used by hackers and found out that they were located in another country.

Determined to catch these criminals before anyone else fell victim to their scamming tactics, Luke contacted local authorities and provided them with all evidence he had gathered.

The police were able to track down the culprits and put an end to their operation thanks to Luke's quick thinking and tech-savviness.

Josh's mother couldn't thank him enough for saving her from potential financial ruin. His actions not only helped her but also prevented many others from falling prey to these scammers' deceitful ways.

From that day on, Luke was known as the hero of Maplewood. But for him, the real reward was knowing that he had outsmarted the bad guys and protected his community from harm.

Luke's parents were proud of their son's bravery and intelligence. They knew that this wouldn't be the last mystery he would solve, as Luke had a natural talent for it. And who knows what other adventures awaited him in the future?

SPEAR PHISHING

Luke was your average 12-year-old boy, living in a quiet suburban neighborhood with his parents and twin sister. He loved playing video games and riding his bike around the block. But little did he know, his world was about to be turned upside down by a mysterious cybercrime.

It all started when Luke's mom received an email from her boss, asking her to urgently transfer funds to a new account for a top-secret project. Being the diligent employee she was, she followed through with the instructions without questioning it. However, this seemingly innocent act would soon lead to chaos.

The next day at school, Luke noticed something strange happening with some of his classmates. They were acting secretive and whispering amongst themselves. He couldn't quite put his finger on it but something felt off.

During lunch break, Luke overheard their conversation and caught snippets of words like "hacking" and "money". His curiosity piqued; he followed them after school to see where they were headed.

To his surprise, they entered an abandoned warehouse on the outskirts of town. Knowing that this could be

dangerous territory for kids like him, Luke decided to investigate further on his own.

He snuck into the warehouse through a back entrance and found himself in front of several computer screens displaying bank accounts being drained one by one. In shock, he realized that these kids had been spear-phishing their way into people's bank accounts using fake emails just like what happened with his mom!

Determined to stop them before they caused any more harm, Luke quickly came up with a plan. Using skills learned from playing detective video games online (something he thought was just for fun), he hacked into their system undetected while also calling the police.

As expected, chaos erupted as soon as the police arrived at the warehouse - with money flying everywhere! The mastermind behind it all tried to escape but thanks to Luke's quick thinking; they were caught and brought to justice.

With the help of Luke's mom, who had been working closely with the police, it was discovered that these kids were being manipulated by a notorious cybercriminal who was using them as pawns in his elaborate scheme. But thanks to Luke's bravery and quick thinking, they were all stopped before causing any major damage.

As for Luke, he became somewhat of a local hero and even received an award from the mayor for his heroic actions. And from then on, he made sure to educate others about the dangers of spear-phishing and how to stay safe online.

From that day forward, everyone knew not to mess with Luke - the 12-year-old boy who solved a social engineering mystery caused by spear phishing!

WHALING

It was a typical summer day in the small town of Maplewood, and Luke couldn't wait to spend his afternoon at the community pool with his friends. But as he walked through the town square, something caught his eye - a large banner hanging outside of the bank that read "Whaling Seminar Today."

Curiosity sparked within Luke as he had never heard of such a thing before. Being an avid reader and always up for learning new things, he decided to attend the seminar instead of going to the pool.

As he entered the bank, he noticed that there were only adults present. He felt out of place but didn't let it bother him as he took a seat in one of the back rows. The speaker began talking about whaling - not whales in the ocean, but rather a type of cyber attack where scammers target high-level executives or employees with access to sensitive information.

Luke's interest peaked when he realized that this type of attack could affect anyone, even people in their small town. Suddenly, all eyes turned towards him as everyone noticed how young he was compared to them.

"Excuse me," said one woman in disbelief. "What are you doing here?"

"I'm just interested in learning more about Whaling," replied Luke confidently.

The speaker nodded approvingly and continued with her presentation while keeping an eye on Luke from time to time.

Afterwards, during Q&A session someone asked if anyone knew someone who fell victim to Whaling attacks? An elderly man stood up and shared how his life savings were stolen because someone posing as his bank manager convinced him over email that there was suspicious activity on his account and needed urgent action taken

Luke's mind started racing with questions. How did they get access? Who could have done this? And most importantly, how can we stop these attacks from happening?

He went home determined to find answers. After hours spent researching online and talking to experts, he discovered that the bank's security system had been hacked by a group of scammers. They used fake emails and social engineering techniques to gain access to sensitive information and steal people's money.

Luke knew he couldn't solve this mystery alone, so he gathered his twin sister Ellie, who were equally curious about the Whaling seminar. Together, they formulated a plan to expose the scammer and bring justice for those who fell victim.

They worked tirelessly, gathering evidence and talking to witnesses until they finally caught the culprit - an ex-employee of the bank who held a grudge against her former employer.

Thanks to Luke's determination and quick thinking, not only was justice served but also awareness was raised in their town about cyber attacks like Whaling. The community came together to tighten their online security measures and protect themselves from potential threats.

The incident may have started as a simple curiosity for Luke but ended up being one of his greatest achievements. He learned that sometimes it takes just one person with determination and knowledge to make a big difference in solving real-world problems. And from then on, Luke became known as "the boy detective" in Maplewood - always ready to solve any mystery that comes his way.

SMISHING AND VISHING

It was a quiet afternoon in the small town of Oakwood. The sun was shining, birds were chirping, and the streets were filled with people going about their day. Among them was 12-year-old Luke, a curious and intelligent boy who always seemed to find himself in the middle of mysterious situations.

As he walked home from school, Luke couldn't help but notice something strange happening around him. People's phones were buzzing constantly and they all had worried looks on their faces. Being naturally curious, Luke decided to investigate.

He followed a group of people into the local coffee shop where he overheard them discussing a recent incident that occurred in town. Apparently, several residents had received suspicious text messages claiming to be from their banks asking for personal information.

Luke's ears perked up at this news as he remembered learning about smishing (a form of phishing through text messages) and vishing (phishing through phone calls) in his technology class last week. He knew that these were

dangerous tactics used by scammers to steal people's identities and money.

Determined to get to the bottom of things, Luke went back home and did some research on his computer. He discovered that many residents had fallen victim to these scams just within the past few days.

Feeling like he needed more evidence before bringing it up with authorities or his parents, Luke decided to take matters into his own hands. With his trusty bicycle as his steed, he rode around town looking for any clues or suspicious activity.

After hours of searching, Luke stumbled upon an abandoned warehouse near the outskirts of town. His instincts told him there was something fishy going on inside so he cautiously made his way towards it.

Peeking through a broken window, Luke saw several men huddled around computers talking on headsets while typing furiously away on keyboards - classic signs of call center operations involved in scamming activities!

Without hesitation, Luke whipped out his phone and secretly recorded a video of the men in action. He also took note of the warehouse's address and quickly reported it to the authorities.

Thanks to Luke's bravery and quick thinking, the police were able to shut down the scam operation and catch those responsible for sending out smishing messages and making vishing calls.

The town was relieved that they no longer had to worry about falling prey to these scams. And as for Luke, he was hailed as a hero by everyone - including his parents who were both proud and amazed by their son's detective skills.

From that day on, Luke became known as "the boy who saved Oakwood from scammers". And he continued using his knowledge for good while always keeping an eye out for any suspicious activity around town.

BAITING

Twelve-year-old Luke was excited to start his summer vacation. After a long year of school, he couldn't wait to spend his days playing video games and hanging out with friends. But little did he know that this summer would be anything but ordinary.

One hot afternoon, Luke's mom asked him to run an errand for her at the local convenience store. As he walked down the street, he noticed a poster on a lamppost that read "Win a trip to Disneyland! Just call this number and answer one simple question!"

Intrigued by the offer, Luke decided to give it a shot. He called the number and heard an automated voice ask him: "What is your favorite color?" Without much thought, Luke answered "blue" and hung up.

A few days later, when his mom asked him about their upcoming trip to Disneyland, Luke was confused. He had completely forgotten about the contest until she showed him an email stating that they had won! His mom was ecstatic but something didn't feel right to Luke.

He remembered hearing about scams where people would bait others into giving away personal information through fake contests. Determined to get to the bottom of it, Luke started investigating.

He went back to the spot where he saw the poster but it was gone. However, using his keen observation skills as well as some help from Google Maps Street View feature, he found another similar poster in a different location.

Luke realized that someone was using these posters as bait and targeting innocent people like himself just for fun or possibly for malicious purposes. He immediately reported it to his parents who then contacted authorities.

With their investigation skills combined with Luke's evidence and testimony, they were able catch the culprit responsible for these fake posters - an ex-employee of a marketing company who wanted revenge against his former employer by causing chaos in their name.

PIGGYBACKING/TAILGATING

Luke was a 12-year-old boy with a knack for solving puzzles. He loved to use his keen observation skills and quick thinking to unravel mysteries around him. This made him quite popular in his neighborhood, as he was always ready to lend a hand when someone needed it.

One day, Luke's neighbor Mr. Johnson came knocking on his door in distress. Mr. Johnson owned a small IT company and had just realized that one of his employees had been duped into giving away sensitive information about their latest project. The employee had fallen victim to piggybacking - an act where an unauthorized person follows someone with legitimate access into a restricted area.

Mr. Johnson explained that the employee had been followed by a stranger who seemed harmless at first but turned out to be after valuable information from their company's database.

Luke immediately took interest in the case and asked Mr.Johnson if he could investigate further. With some hesitation, Mr.Johnson agreed and gave Luke the necessary details including CCTV footage of the incident.

After carefully studying the footage, Luke noticed something peculiar - every time someone entered or left the building, there was always another person following closely behind them without swiping their ID card for entry.

With this information, Luke devised a plan to catch the culprit red-handed. He convinced Mr.Johnson to hold an emergency meeting with all employees regarding security protocols and announced that they would conduct random checks throughout the building.

On the day of the meeting, while everyone gathered in one room for discussion, Luke snuck out unnoticed and stationed himself near one of the restricted areas where tailgating commonly occurred.

Sure enough, within minutes he spotted two individuals trying to enter through security gates without proper authorization - one posing as an employee while being escorted by another real employee who didn't suspect anything amiss.

Using his quick reflexes, Luke alerted security personnel who apprehended both suspects before they could cause any harm or steal any information.

After the incident, Mr. Johnson was grateful to Luke for solving the mystery and preventing any further security

breaches in his company. He even offered Luke a job as a junior detective at his IT firm when he turned 18.

From that day on, piggybacking became a thing of the past in their neighborhood. And Luke's reputation as an ace detective only grew stronger, making him the go-to person for any puzzling mysteries in town.

PRETEXTING

It was a sunny day in the small town of Oakwood. The birds were chirping, the flowers were blooming and everyone seemed to be going about their daily business. But little did they know, a mysterious social engineering case was about to unfold.

Luke was a 12-year-old boy who loved solving mysteries. He had an eye for detail and an insatiable curiosity that often got him into trouble. On this particular day, he was walking home from school when he overheard two men talking on their phones.

"I need those bank account details ASAP," one man said impatiently.

"Don't worry, I'll get them through pretexting," the other replied with a sly grin.

Luke's ears perked up at the unfamiliar word 'pretexting'. He quickly pulled out his phone and searched for its meaning. To his surprise, it meant lying or deceiving someone in order to obtain sensitive information.

His mind raced with possibilities as he followed the two men discreetly. They entered a nearby coffee shop and Luke decided to follow them inside. As soon as they sat down at a table, Luke hid behind a newspaper pretending to read while secretly listening in on their conversation.

He heard them discussing various schemes involving pretexting- from fake charities to false identities used for scamming people out of money. This made Luke angry- how could these grown men take advantage of innocent people like that?

Determined to stop them, Luke went straight home and told his parents everything he had witnessed. His father immediately called the police while Luke gave them all the information he had gathered.

The next day, there were news articles floating around about how several scams had been uncovered thanks to an anonymous tip-off from a young boy named Luke who had overheard conversations at a coffee shop.

The entire town was buzzing with excitement over this brave young detective who helped bring justice to those who preyed on others through pretexting.

Luke's name was now known by everyone in Oakwood and he even received a special award from the mayor for his

bravery and quick thinking. From that day on, Luke became known as the town's very own Sherlock Holmes.

HONEYTRAPS

Luke was a typical 12-year-old boy living in the bustling city of New York. He loved spending his free time playing video games and hanging out with his friends. However, little did he know that his life was about to take an unexpected turn.

It all started when Luke's dad got a new job at a big tech company. His family had to move into a high-rise building in the heart of the city, where most of the employees also lived. The first day at their new apartment, Luke explored every nook and cranny, including the rooftop terrace.

While up there, he stumbled upon something peculiar - a strange-looking device hidden behind some potted plants. Curiosity getting the better of him, Luke decided to investigate further and found out that it was actually a sophisticated surveillance camera!

Without wasting any time, Luke went straight to his parents and told them what he had discovered. They were shocked but didn't seem too concerned until they received an anonymous letter threatening to expose their secrets if they didn't comply with certain demands.

Luke's dad immediately reported it to his boss who brushed it off as some prank by disgruntled employees. But things only got worse from there on out - more letters arrived and this time containing photos and videos taken from inside their apartment! It was clear that someone was watching them closely.

Feeling helpless and scared for their safety, Luke's parents turned to him for help since he seemed so interested in figuring things out. With nothing else left for them to do, they gave him permission to use his computer skills (learned from endless hours of gaming) to trace down whoever was behind these threats.

Using social engineering techniques that he learned online (against his parent's wishes), Luke managed not only traced back those letters but also identified who sent them – one of their neighbors!

Turns out she had been hired by another tech company competitor as part of an elaborate honeytrap scheme to extract confidential information from employees. She had been planting surveillance devices in several apartments, and Luke's family was one of her targets.

With the evidence collected by Luke, the neighbor was arrested, and their secrets were safe once again. His parents were amazed at how clever and resourceful their son had been in solving this mystery that even adults couldn't figure out.

From then on, Luke became known as the "12-year-old detective" and his skills were highly sought after by many companies looking to enhance their security measures. And although he got grounded for disobeying his parents' rules about using computer skills without permission, they couldn't be prouder of him for saving them from a potential disaster.

Luke learned an important lesson – that sometimes curiosity can lead you down dangerous paths but with responsibility and quick thinking, you can also use your knowledge for good.

SCAREWARE

It was a sunny afternoon in the small town of Maplewood. The birds were chirping, children were playing and everything seemed calm and peaceful. But little did anyone know, a sinister plot was about to unravel.

As Luke walked home from school, he noticed something strange on his computer screen. A pop-up appeared with a flashing red warning sign that read "Your computer has been infected with viruses! Click here to remove them now!" Being only 12 years old, Luke panicked and clicked on the button without thinking twice.

Suddenly, his screen went black and a message appeared stating that all his files had been encrypted and he needed to pay $500 in order to get them back. This was known as Scareware - malicious software designed to trick people into paying money for fake virus removal services.

Luke's heart sank as he realized what had happened. He knew his parents would be furious if they found out he fell for such an obvious scam. But instead of giving up hope, Luke decided to take matters into his own hands.

He used his advanced coding skills (which he learned from watching YouTube tutorials) to track down the source of the

scareware. With each line of code typed on his keyboard, he uncovered more clues leading him closer to the culprit.

After hours of digging through lines of code and online forums, Luke finally found the mastermind behind it all - Mr.Carter, their next-door neighbor who also happened to own a computer repair shop in town.

With this evidence in hand, Luke bravely approached Mr.Carter's shop where he saw dozens of computers being serviced at once. Feeling nervous but determined, Luke confronted Mr.Carter with what he had discovered.

To everyone's surprise (especially Luke's), Mr.Carter broke down in tears confessing that due to financial struggles with his business; he resorted to using scareware tactics as means for extra income.

Feeling sympathetic towards their neighbor, Luke's parents decided not to press charges. But they made sure Mr.Carter paid back all the victims he had scammed.

From that day on, Maplewood became a safer place and Luke gained recognition as the young hero who solved the social engineering mystery caused by scareware. And as

for Mr.Carter, he learned his lesson and never resorted to such deceitful tactics again.

WATERING HOLE ATTACK

It was a typical Saturday afternoon in the small town of Oakwood. The sun was shining, birds were chirping, and people were out enjoying their weekend activities. But little did they know, a sinister plot was about to unfold.

Luke, a 12-year-old boy with a curious mind and an eye for details, was riding his bike around town when he stumbled upon an odd sight. A group of people gathered around what seemed to be a newly opened park called "The Watering Hole". Luke's curiosity got the best of him as he decided to stop and take a closer look.

As he approached the crowd, Luke noticed that everyone seemed dazed and confused. They were all staring at their phones with blank expressions on their faces. It didn't take long for him to realize that something wasn't right.

Being the tech-savvy kid that he is, Luke knew about cyber attacks and how hackers could use social engineering tactics to deceive people into giving away sensitive information. He quickly checked his phone and saw multiple notifications from various social media accounts promoting The Watering Hole park opening.

Realizing that this could be a watering hole attack - where hackers set up fake websites or events to lure unsuspecting victims into giving away personal information - Luke sprang into action.

He discreetly made his way through the crowd, observing each person closely until he found one man who seemed particularly suspicious. This man had been walking around with some sort of device hidden under his jacket while constantly checking his phone.

Without hesitation, Luke approached the man and asked if everything was okay. The man nervously replied yes but before he could say anything else, Luke grabbed hold of the device under his jacket which turned out to be a portable wifi router connected to all the devices in the vicinity.

With evidence in hand, Luke ran towards The Watering Hole's main office where he alerted security about what had happened. It turned out that the man was a hacker who had set up the fake park opening to steal people's personal information.

Thanks to Luke's quick thinking and detective skills, disaster was averted. The crowd slowly snapped out of their daze and security quickly shut down the wifi router, preventing any further data theft.

The town of Oakwood hailed Luke as a hero for his bravery and clever thinking. And from that day on, he became known as the "Watering Hole Detective". But most importantly, Luke reminded everyone about the importance of staying vigilant against cyber attacks and not falling prey to social engineering tactics.

ADVICE FROM LUKE

I may only be twelve years old, but when it comes to social engineering in cybersecurity, I'm an expert."

Remember, this advice is important for people of all ages. Cybersecurity affects everyone, so it's important to stay informed and be cautious when using technology. And if you ever have any doubts or concerns about a suspicious message or website, don't hesitate to ask an adult for help.

With technology becoming more advanced every day, cyber attacks are becoming more and more common. So let's review some of the most common types of cyber attacks used by the criminals and how to protect ourselves from them.

Phishing

Phishing is a type of cyber attack where scammers try to trick you into giving out your personal information, such as passwords or credit card numbers. They usually do this through fake emails, messages or websites that look like they are from a legitimate source. It's important to remember to never click on links or open attachments from suspicious sources, as they could be phishing attempts.

Spear Phishing

Spear phishing is a more targeted version of phishing where scammers use personal information about their victims to make the attack seem more legitimate. For example, they may use your name, job title, or company name to gain your trust. It's important to be cautious when sharing personal information online and always verify the source of any suspicious emails or messages.

Whaling

Whaling is a type of spear phishing attack that specifically targets high-profile individuals, such as CEOs or celebrities. These attacks often involve convincing the victim to transfer large sums of money or sensitive information. It's important to always be on guard, even if you think you are not a target for such attacks.

Smishing & Vishing

Smishing and vishing are similar to phishing, but they use text messages or phone calls instead of emails. Scammers will try to trick you into giving out your personal information through these methods, so it's important to always be cautious and not give out any sensitive information over the phone or through text messages.

Baiting

Baiting is a type of cyber attack where scammers lure their victims with an enticing offer, such as free downloads or prizes. However, the download or prize is usually infected with malware that can compromise your device or steal

your personal information. It's important to never download anything from untrusted sources and to be cautious of offers that seem too good to be true.

PiggyBacking/Tailgating

Piggybacking or tailgating is when someone without proper authorization follows an authorized person into a restricted area. This can happen physically, such as in an office building, but it can also happen digitally through shared passwords or accounts. It's important to never share your passwords or give anyone access to your accounts without proper authorization.

Pretexting

Pretexting is a type of social engineering attack where scammers create a fake scenario to gain the trust of their victim and trick them into giving out personal information. For example, they may pretend to be from a legitimate organization and ask for your personal information to "verify" your identity. It's important to be cautious of anyone asking for your personal information and to always verify the credibility of their request.

HoneyTraps

Honey traps are a type of cyber attack where scammers use attractive individuals or fake profiles to lure their victims into revealing sensitive information or downloading malware. It's important to be cautious when interacting

with strangers online and to never share personal information or click on links from suspicious sources.

Scareware

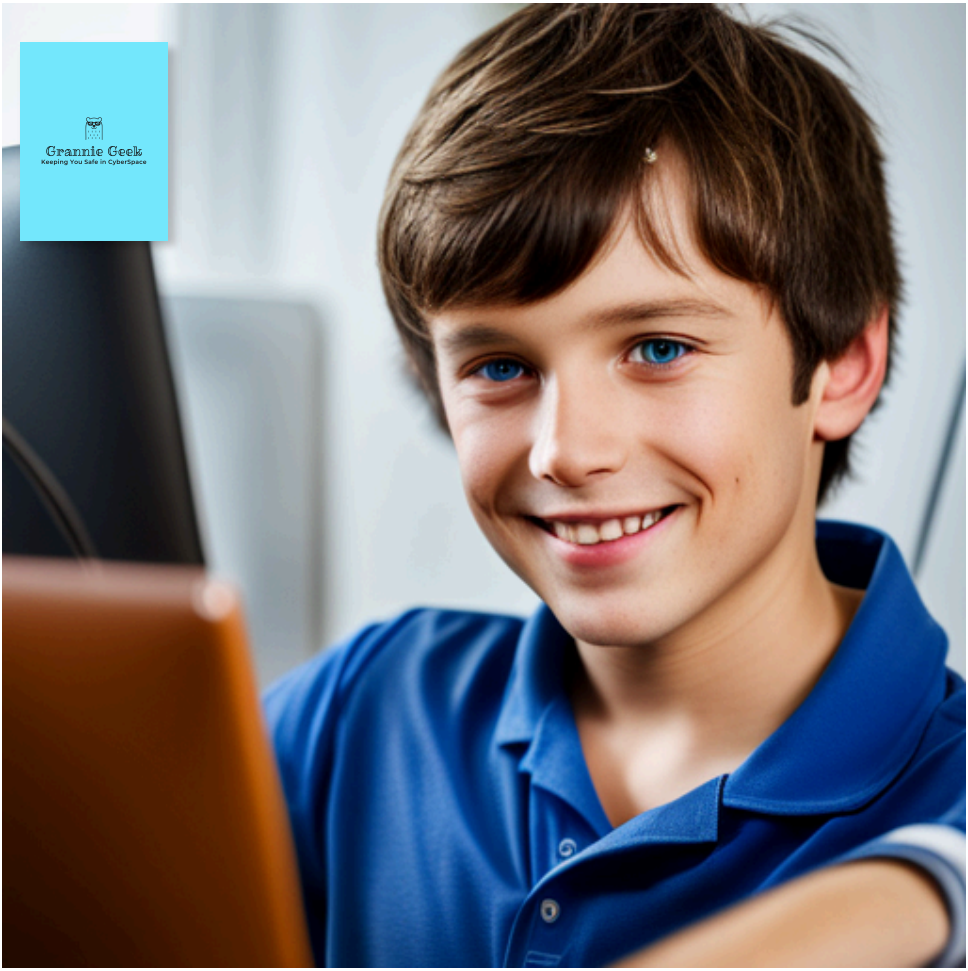
Scareware is a type of cyber attack where scammers use pop-up messages or fake antivirus software to trick their victims into believing that their device has been infected with malware. They then offer a solution for a fee, but in reality, they are just trying to steal your money. It's important to always use legitimate antivirus software and never fall for scare tactics.

Watering Hole Attack

A watering hole attack is a type of cyber attack where scammers infect a popular website with malware, knowing that many people will visit that site. When users visit the infected site, their devices become compromised with malware without their knowledge. It's important to keep your devices and software up to date to prevent these types of attacks.

So there you have it, some of the most common types of cyber attacks and how to protect yourself from them. Remember, always be cautious when sharing personal information online or clicking on links from suspicious sources. Stay safe out there!

But don't worry!



GrannieGeek.com

ISBN: 978-1-7372783-2-0