For my son, Tyler.

Can we go Phishing, Dad?
Author: Cody Williams
Started writing: 16/07/2024

Contents:

----

chapter 1. Introduction

----

importance of cyber security.

In such a rapidly evolving technological world, staying up to date on cybersecurity trends and understanding their impact on our families is crucial for navigating today's digital age. A lack of awareness is a major factor in falling victim to cybercrime. This book aims to highlight important cyber security issues that affect countless people each year and provide tips on passing this knowledge to the next generation of internet users.

why it's important to educate children about it.

Educating children about cybersecurity is crucial, as they are often major targets for scammers and hackers due to their lack of knowledge and innocent curiosity. As kids learn to navigate the internet in our increasingly cyber-dependent world, education should be our first line of defence. This preventative measure is not just about protecting them—it's about equipping them with the knowledge to navigate the digital world safely. By teaching them about the risks and how to avoid them, we can significantly reduce their vulnerability to cybercrime and potentially save them, or someone they know, from falling victim to these digital threats.

Chapter 2
Understanding the Internet

First let's understand that no organisation or person alive owns the internet. It doesn't really work like that at all. The *internet* is a bunch of clients communicating with servers and amongst themselves. Your phone? That's a client and when you open your internet browser and type www.google.com, your browser is attempting to connect your client to a server (google). Your phone basically sends a tiny 'packet' of information that says something like "Hey can I get access to google.com?". That server essentially then sends back a document in the form of a website. Sure there's a lot more too it then that, but we're here to pass on cyber security knowledge, not learn about computer science.

Once you've established that you can't physically own the internet; you can then understand that it would be next to impossible to fully control something that is just a series of devices that come and go as they communicate with each other. If anyone could use their client to send packets to another client or server, how will we know exactly when or where the next client will pop up? It is then easy to see how it might be hard to stop the bad guys from causing damage with clients and servers of their own as they could be anyone at any time.

Chapter 3
The Good Guys VS the Bad Guys

Since the dawn of the internet, an ongoing war rages between good and evil. The good guys, doing their best to build secure systems that are robust and usable to the best of their ability. Then we have the bad guys, those whose sole purpose is to break into those systems, manipulating weaknesses in code and creating chaos for everyday people. In Cybersecurity, we typically label these as the blue team (The good guys) and red team (The bad guys). The idea is simple enough without labels when you see there are essentially 2 sides to this never-ending battle that has plagued cyber security professionals since the beginning of the technology age.

Hackers, script kiddies, scammers… Whatever you choose to name them, these are the bad guys that cause harm or damages to systems and people for their own benefit. Whether this is for financial gain like credit card fraud, or political motivation such as government sponsored hackers that attempt to break into rival countries systems to manipulate the views of their people.

##Include reference about the cost of cybercrime/hackers.

The Blue team is constantly trying to counter these threats by rolling out software updates to fix bugs or monitoring systems to detect intruders. It is a never-ending cycle of, deploy a program, the program gets hacked and is then updated to prevent that threat from reoccurring.

Chapter 4
What is Phishing?

Normally, if your child approaches you and asks, “Can we go fishing?”. They’ll surely mean casting out a line and bait into a bed of water… but what about Phishing? Phishing is a term used in IT that refers to fraudulently cloning a website or company to fool victims into clicking a malicious link or giving away their personal information via dodgy emails or text messages to your phone.

I know what you’re probably thinking, *who could be foolish enough to fall for a fake website?* Truthfully, many people. In fact, in 2023 alone, *Phishing* dealt around $26 million in financial losses to victims with over 100,000 reports of phishing-related crime (SBS News, 2024).

References

SBS News. (2024). $481m in losses and 302,000 complaints: *The scams hitting Australians hard.* ***https://www.sbs.com.au/news/article/481m-in-losses-and-302k-complaints-the-scams-hitting-australians-hard/hg52ignc8***