1. Record Nr. UNINA9910731463603321

Autore	Oles Nicholas
Titolo	How to Catch a Phish : A Practical Guide to Detecting Phishing Emails / / by Nicholas Oles
Pubbl/distr/stampa	Berkeley, CA : , : Apress : , : Imprint : Apress, , 2023
ISBN	9781484293614 1484293614
Edizione	[1st ed. 2023.]
Descrizione fisica	1 online resource (153 pages)
Disciplina	005.82
Soggetti	Phishing - Prevention Electronic mail messages - Security measures
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Note generali	Includes index.
Nota di contenuto	Chapter 1. How Email Works -- Chapter 2. Phishing Tactics and Techniques -- Chapter 3. PICERL Process explained -- Chapter 4. Analyzing Message Content -- Chapter 5. Links -- Chapter 6. Attachments -- Chapter 7. Log Searching and Response -- Chapter 8. Remediation and Lessons Learned.
Sommario/riassunto	Learn how to detect, analyze, and respond to phishing emails, the top infection vector used by cybercriminals. The repeatable process described in this book has been cultivated and tested in real-life incidents and validated across multiple threat landscapes and environments. Every organization and individual with an email account is susceptible to deceptive emails sent by attackers with nefarious intentions. This activity, known as phishing, involves an attacker attempting to lure individuals into providing sensitive information or performing a predetermined action. Attacks vary in sophistication, but the core skills and process to detect, analyze, and respond to a suspicious message does not change. Attackers have preyed on victims with convincing and not-so-convincing phishing emails to gain initial footholds into networks around the world for over 30 years. This attack method has been rapidly growing in popularity and continues to be the number one method that organizations and individuals struggle to defend against. Regardless of what any vendor or organization will tell you, no infallible tool exists to eliminate this threat completely. This

book teaches you how to analyze suspicious messages using free tools and resources. You will understand the basics of email, tactics used by attackers, and a repeatable process to systematically analyze messages and respond to suspicious activity. You Will Learn How to: Safely save email messages as attachments for analysis Identify what information is in an email header Review header information and extract key indicators or patterns used for detection Identify signs of a suspicious or malicious email message Detect the tactics that attackers use in phishing emails Safely examine email links and attachments Use a variety of free and simple tools to analyze email messages.