Ebookecm.it è un servizio Bookia srl, Piazza Deffenu 12, 09125 Cagliari, P.I. 03787400922

CYBERSECURITY PER PROFESSIONISTI SANITARI

Abstract lungo:
Il libro "Cybersecurity per professionisti sanitari" è una guida completa alla sicurezza informatica per tutti i professionisti e le professioniste della salute. Il libro copre una vasta gamma di argomenti, tra i quali le minacce alla sicurezza informatica per i professionisti sanitari, la creazione e gestione di password sicure, la protezione dei dati dei pazienti, la prevenzione e il riconoscimento di phishing e virus anche su telefono cellulare, l'utilizzo della crittografia per proteggere i dati sensibili e la sicurezza nell'utilizzo di dispositivi medici collegati alla rete sempre più spesso avviene attraverso la telemedicina e l'e-helath. Il libro è scritto in un linguaggio comprensibili anche ai non addetti ai lavori e contiene numerosi esempi e suggerimenti pratici. È un prezioso strumento per tutti i professionisti sanitari che desiderano proteggere i propri pazienti e le proprie organizzazioni dalle minacce alla sicurezza informatica. Un testo sintetico e chiaro, ma completo ed essenziale per tutti i professionisti sanitari che desiderano proteggere i propri pazienti e le proprie organizzazioni dalle minacce legate alla sicurezza informatica.

Abstract breve (160 caratteri):
Un testo sintetico e chiaro, ma completo per tutti i professionisti sanitari che desiderano proteggere i propri pazienti e le proprie organizzazioni dalle minacce legate alla sicurezza informatica

Programma degli argomenti

1. Introduzione

2. Il rischio cyber nella sanità

3. Le minacce in ambito sanitario

3.1 Perché le strutture sanitarie?

3.2 Best practice in ambito sanitario

4. La minaccia

4.1 Phishing e Spoofing

4.2L'infezione da malware.

4.3Ricapitolando

5. Le password e la loro gestione

5.1 Password debole

5.2 Utilizzo della stessa password.

5.3 Come scrivere password sicure

5.4 Autenticazione a più fattori

5.5 Ricapitolando

6. Phishing

6.1 Come avviene un attacco di phishing?

6.2 Spear Fishing

6.3 Come difendersi dal phishing

6.4 Riconoscere i nomi di dominio

6.4.1 Facciamo degli esempi:

6.5 Esempi di phishing

6.5.1 La mail da Intesa Sanpaolo

6.5.2 La richiesta di riscatto:

6.5.3 Phishing Amazon

6.5.4 Buoni Alitalia

6.6 Ricapitolando

7. Social Engineering

7.1 Esempio di attacco

7.2 Tecniche di Social engineering

7.3 Come proteggersi.

7.4 Ricapitolando

8. Shopping on line

8.1 Paypal

8.2 Ricapitolando

9. Accesso alle reti Wireless

9.1 Ricapitolando

10. Supporti rimovibili

10.1 Proteggersi da USB infette?

10.2 I dispositivi USB criptati

10.3 Ricapitolando

11. App malevoli e truffe

11.1 Tipologie di malware più utilizzate

11.1.1 Advertising App

11.1.2 Fleeceware

11.1.3 Bankers

11.2 Cos'è il "Sim swap fraud"

11.2.1 Come difendersi

11.3 Ricapitolando

12. Capire se lo smartphone è stato infettato

12.1 I principali indicatori da controllare:

12.1.1 Verificare il consumo della batteria

12.1.2 Verificare il consumo dei dati

12.1.3 Surriscaldamento del dispositivo

12.1.4 Arresti anomali delle applicazioni

12.1.5 App mai viste prima

12.1.6 Popup indesiderati

12.2 Ricapitolando

13. I dispositivi medicali connessi

13.1 Ricapitolando

14. Riflessioni finali

PAGG. 100

Responsabile Scientifico e Relatore

Antonio Capobianco
Si laurea con lode in informatica nel 1993 e nell'anno seguente fonda Fata Informatica, società della quale è tuttora il CEO. Docente universitario nel corso di Cybersecurity Threats Analysis presso l'Università degli studi Guglielmo Marconi ed esperto in cybersecurity ha gestito numerosi progetti nel campo della sicurezza IT e gestione di infrastrutture complesse. Nel 2017 ha creato il brand CybersecurityUP, BU di Fata Informatica che eroga servizi a valore aggiunto nel campo della Cybersesecurity. Ha inoltre progettato e diretto lo sviluppo di Sentinet3, l'unico sistema di monitoraggio IT sviluppato in Italia ed inserito nella "Marketing Guide for IT monitoring tools" di Gartner.