



Fișa de exerciții privind Mobile Money

MODUL 2

Exercițiul 1

Joacă și învață Chestionar

Durata estimată a exercițiului

10 min

Materiale

Dispozitiv cu acces la internet pentru clarificarea dubiilor

Hârtie și stilou

Instrucțiuni

Pe pagina următoare ai 5 întrebări despre securitatea și siguranța online!

Încercuiește întrebările și găsește răspunsurile cu explicații pe pagina a 3-a - fără să tragi cu ochiul!

:-)



1. Care este cea mai comună metodă de transmitere a virușilor?

- A. Email
- B. Mesagerie instantanee
- C. Descărcare de pe internet
- D. Portable media

2. Care dintre următoarele ar fi cea mai bună parolă?

- A. SecretulMeu
- B. lw2c^tILV
- C. Abc123
- D. George1234

3. Sora dvs. vă trimite un e-mail la serviciu cu un screen saver despre care spune că v-ar plăcea. Ce ar trebui să faci?

- A. Descărcați-l pe computer, deoarece provine dintr-o sursă de încredere.
- B. Transmiteți mesajul altor prieteni pentru a-l partaja.
- C. Sunați la IT și rugați-i să vă ajute să-l instalați
- D. Ștergeți mesajul.

4. Atunci când primiți un e-mail de la un contact necunoscut care are un atașament, ar trebui să:

- A. Deschideți atașamentul pentru a-i vizualiza conținutul
- B. Să ștergeți e-mailul
- C. Transmiteți e-mailul colegilor dvs. pentru a le permite să deschidă mai întâi atașamentul
- D. Transmiteți e-mailul către contul dvs. personal de e-mail astfel încât să îl puteți deschide acasă



1. Care este cea mai comună metodă de transmitere a virușilor? ?

A. E-mail

E-mailul este cea mai frecventă metodă de transmitere a virușilor. Infractorii cibernetici folosesc adesea e-mailul ca vector pentru a distribui programe malware. Aceste e-mailuri pot părea a proveni din surse de încredere, ceea ce le face deosebit de periculoase. Odată ce destinatarul deschide atașamentul sau face clic pe link, virusul poate fi descărcat și executat pe dispozitivul său.

2. Care dintre următoarele ar fi cea mai bună parolă?

B. lw2c^tILV

Pentru că respectă principiile cheie ale creării unei parole puternice:

Complexitate: Include un amestec de litere majuscule, numere și caractere speciale, ceea ce o face dificil de ghicit sau de spart prin forță brută de către atacatori.

Lungimea: Este suficient de lungă, ceea ce adaugă un alt nivel de securitate. Parolele mai lungi sunt, în general, mai greu de spart.

Impredictibilitate: Parola nu include cuvinte sau modele ușor de ghicit, care sunt fie comune, fie simple, fie legate de utilizator.

3. Sora dvs. vă trimite la serviciu un e-mail cu un screen saver.

D. Ștergeți mesajul.

4 riscuri mari:

1. Unele screen saver-uri conțin viruși.
2. Apăsând pe un link malițios poate infecta un computer.
3. Adresele de e-mail pot fi falsificate, astfel încât, doar pentru că e-mailul spune că este de la cineva cunoscut, nu puteți fi sigur de acest lucru fără a verifica.
4. Unele site-uri și linkuri par legitime, dar sunt de fapt farse menite să vă fure informațiile.

Fiți în siguranță și bucurați-vă de lumea digitală!