PAG101 - Moneta e Pagamenti online

Domande aggiuntive | Week 4 – Rischi e sicurezza

1. **Rispondi alle seguenti domande.**
   Esistono varie tipologie di truffe: ma qual è l'obiettivo dei truffatori? Cosa devi fare per mantenere le tue informazioni personali al sicuro?

   _____
   _____
   _____
   _____

2. **Metti in ordine la frase, inserendo il numero corrispondente davanti a ogni frase.**

- ☐ rispondere subito ma verifica il contenuto della mail, controllando la presenza di errori di ortografia e di grammatica;
- ☐ La truffa più diffusa è il phishing, che
- ☐ link a un sito clone di quello della Banca. Per
- ☐ lo stesso logo e le stesse modalità di comunicazione della banca,
- ☐ un indirizzo di posta elettronica e un pretesto verosimile. Spesso fanno leva su
- ☐ rendere verosimile la richiesta, i truffatori utilizzano spesso
- ☐ un messaggio allarmistico del tipo ''il tuo conto è stato bloccato per un attacco hacker'' e ti
- ☐ consiste nella richiesta via mail di inserire i tuoi dati personali attraverso un
- ☐ se hai dubbi, chiama la tua banca. Inoltre, tieni aggiornati browser e antivirus.
- ☐ chiedono di riattivarlo. Per evitare di cadere in trappola puoi prendere alcuni accorgimenti. Non

3. **Completa il seguente testo con gli esempi richiesti.**
   Quando fai un pagamento online la normativa Europea ha introdotto la cosiddetta autenticazione forte o SCA che si basa su almeno due o più fattori di sicurezza:
   a. Qualcosa che soltanto tu conosci (per esempio _____)
   b. Qualcosa che tu possiedi (per esempio _____)
   c. Qualcosa che dimostra che sei proprio tu (per esempio _____)

4. **Rispondi alla seguente domanda.**
   Cosa deve fare l'intermediario per non rimborsarti?

   _____
   _____
   _____
   _____