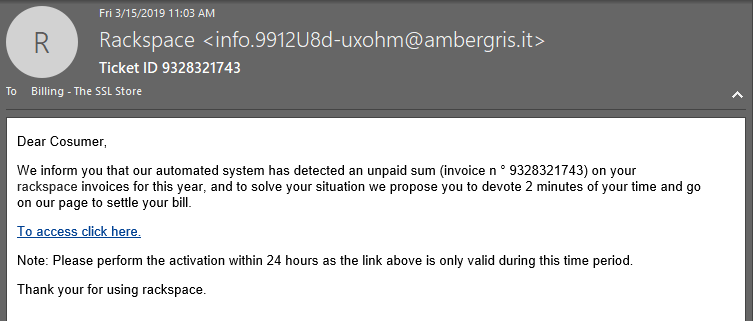
Road Warrior IT Security Training Exam

Multiple Choice. Read each question and answer carefully and select the BEST answer:

1. You are less likely to experience an IT security incident when travelling:
   1. True
   2. False
2. Why is IT Security important?
   1. We have a duty
   2. Data breaches cost a lot of money in downtime and fines
   3. It’s the law
   4. All of the above
3. Cyber criminals are really only looking for bank account details.
   1. True
   2. False
4. How can you better protect your user account?
   1. Use a complex password
   2. Use Multi-Factor Authentication
   3. Change your password when you think you’ve been compromised
   4. All of the above
5. Mutli-Factor Authentication is defined as:
   1. Having multiple people know your password in case you forget it.
   2. Being challenged to approve a login after providing your password.
   3. Not using a password when logging in.
6. Which of the following is NOT correct when it comes to data security?
   1. Device encryption provides no protection to sensitive data on a device.
   2. You should always secure your mobile phone with a passcode.
   3. You should never leave your laptop unattended.
   4. Only allow someone you know and trust to access your computer.
7. Which of the following is a “red flag” that your account/identity may have been compromised?
   1. You have lost access to your online accounts.
   2. You stop receiving a utility bill.
   3. You get an e-mail from a friend/colleague that you sent them a strange e-mail.
   4. All of the above.
8. Phishing is a type of social engineering.
   1. True
   2. False
9. What is phishing?
   1. A great way to relax and unwind after a long week of auditing.
   2. At attack vector designed to steal your information by impersonating someone or something.
   3. An attack vector designed to hack into a computer system using a sophisticated computer program.
10. How can you identify a phishing e-mail?
    1. By hovering over links to see where they take you.
    2. By examining the sender and recipients.
    3. Downloading and opening attachments.
    4. Both A & B
11. Look at the following phishing e-mail. Please provide 2 red flags that the message is not legitimate.



* 1. [Type an answer here]
  2. [Type an answer here]

1. What is Link Manipulation?
   1. A sophisticated phishing attack.
   2. A mistyped web address that resembles a correct address.
   3. A link to a seemingly legitimate website at time of send, but after a few days the website starts hosting malware.
   4. All of the above.
2. Which of the following is NOT a technique of Social Engineering?
   1. Using your publicly available information in order to fool into thinking something is legitimate.
   2. Straight up lying to you or someone to get information.
   3. Phishing
   4. Connecting to a mobile hotspot.
3. When a security incident occurs, you should:
   1. Ask if a data breach occurred.
   2. Disconnect from the Internet.
   3. Call the SQA IT Manager.
   4. All of the above.
4. Keeping your computer operating system and applications up to date is a great way to maintain data security.
   1. True
   2. False
5. Which of the following Tips & Tricks are the most important to you?
   1. Use a secure password manager.
   2. Use a good up-to-date antivirus.
   3. Avoid Unsecure WiFi and opt to use a mobile hotspot if you have one.
   4. Use your Smithers e-mail for business-related activity, not for coupons or fantasy football.
   5. Stay Vigilant
6. One thing I would like to learn more about IT security is:
   1. [Type an answer here]