**Quiz 1 – Quick Test – Just How Safe Are You?**

1. **Passwords should have a lifespan; how often should passwords be changed?**
   1. Where security is a concern, good values are 30, 60, or 90 days
   2. Where security is less important, good values are 120, 150, or 180 days
   3. A and B
   4. None of those

**Answer: c**

1. **You are leaving town on business, so you pick up a laptop from customer support. The technician that issued you the laptop also gave you a user name and password on a sticky note, what should you do now?**
   1. Attach the sticky note to the laptop screen
   2. Hide the password inside the carrying case
   3. Commit the password to memory and destroy the note
   4. Save the password on a removable device or 'flash' memory stick

**Answer: b**

1. **It’s the middle of the afternoon and you have a lot of work to get done before you can go home and you receive a call from someone identifying themselves as IT support, the technician states they need your password to remotely deploy a new software package for you, what should you do?**
   1. Yes, give them the password
   2. No, do not give them the password

**Answer: b**

1. **A customer service representative has just called you saying that your credit card is about to expire, he or she asked you to provide your account information and personal information in order to verify your account and to renew your credit card without telling you from what bank he or she came from. What should you do?**
   1. Ask the customer representative what bank or company he or she came from.
   2. Verify your credit card if it really expired because expiration dates are placed on credit cards
   3. Don’t give out your personal information and credit card information yet if you don’t have enough information about the customer service representative yet or about the bank.
   4. All of the above

**Answer: d**

1. **The first step in Security Awareness is being able to \_\_\_\_\_\_\_\_ a security threat.**
   1. Avoid
   2. Recognize
   3. Challenge
   4. Log

**Answer: b**

**Quiz 2 - What is Information Security**

1. **While visiting your favorite website for downloading the Firefox browser, a popup appears that says “You just won 100,000 US dollars! Click this link to claim your prize”, what should you do?**
   1. Ignore that popup and just download the Firefox browser.
   2. Click the popup and claim your prize.
   3. Report the popup and the details to the website administrator and don’t download the Firefox browser.
   4. Share the link to your friends, classmates and colleagues so that they could also claim the prize because sharing is caring.

**Answer: c**

1. **Your college best friend has just sent you a chat in Facebook and sent with a link. The link is a shortened URL for example https://goo.gl/n0NS3cuR3, what should you do?**
   1. Click the link because it shouldn’t be malicious since he/she is your best friend after all. There is nothing to worry about.
   2. Do not click the link and try to check the URL using an online tool that checks where it really takes you.
   3. Contact your local Computer Emergency Response / Readiness Team because it may contain malicious software.
   4. Install antivirus software, then click the link.

**Answer: b**

1. **Your organization is retiring many computers, many of which processed sensitive information; the plan is to delete all the data from the hard drives and donate them to a charitable institution. Is deleting all data from the hard drives an acceptable media sanitization method?**
   1. Yes
   2. No

**Answer: b**

1. **During a conversation with some colleagues you learn your organization is exchanging sensitive personal information outside your organization via unencrypted email, is this method of transferring sensitive information acceptable?**
   1. There are many types of sensitive information such as PII, HIPAA, FTI, PCI, etc., and all are governed by State and Federal regulations and policies; regardless the type, all require encryption when moved electronically from one place to another such as email.
   2. No, while email can be used to send sensitive information, it is not acceptable to transfer any sensitive information without encryption

**Answer: a**

1. **On your personal laptop you have been using some of the same computer programs for years. One of your friends, who is an expert in security, noticed that one of your programs has long been discontinued by the manufacturer. Your friend told you that this old and discontinued software exposes your computer to serious security threats. Among these threats your friend mentioned…..**
   1. The Dark Net
   2. Malicious Software
   3. Privacy Invasions

**Answer: b**

**Quiz 3 - Be Prepared for Social Engineering**

1. **You receive an e-mail from your bank telling you there is a problem with your account. The e-mail provides instructions and a link so you can log in to your account and fix the problem. What type of attack could this be?**
   1. Social Engineering
   2. Browser Hijacking
   3. Debugging

**Answer: a**

1. **One of your friends has recently been a victim of a social engineering attack since someone has stolen her username and password for accessing her work email. This name, ‘social engineering’ looks quite strange to you as it puts together engineering with social issues. What does social engineering mean in a security context?**
   1. Building systems that are easy to use for society.
   2. It is a form of social deception focused on information gathering, fraud, or system access
   3. Someone uses social networks for stealing personal data.

**Answer: b**

1. **You receive an email in your inbox from an email address that doesn’t look familiar; however the body and subject line says it is from your bank. The email has a link to change your current password due to security issues. Upon clicking the link you get a strange message indicating the security certificate is invalid. You close the web page because you usually never get this certificate message therefore you shouldn’t trust the page. This is an example of which of the following:**
   1. Virus Alert
   2. Phishing
   3. Firewall Issues
   4. Directory Harvesting

**Answer: b**

1. **You receive an email reply from a vendor with whom you conduct business routinely. The email arrives with a Microsoft Office attachment, while attempting to open the attachment you are presented with a message box warning that the document has macro’s, and asking whether or not to enable them, what should you do?**
   1. Select NO (do not use macro’s) and open the document
   2. Select YES (enable the document macro’s) and open the document
   3. Reply to the email asking them to verify the document includes macro’s
   4. Delete the email because the email you received was in reply to an email you never sent.

**Answer: d**

1. **It’s the middle of the afternoon and you have a lot of work to get done before you can go home and you receive a call from someone identifying themselves as IT support, the technician states they need your password to remotely deploy a new software package for you, what should you do?**
   1. Yes, give them the password
   2. No, do not give them the password

**Answer: b**

**Quiz 4 - Understand the Difference Between Security, Privacy and Anonymity**

1. **You are in the process of entering sensitive information into your system when you are called to attend a meeting, you don’t bother logging off or locking your computer because local policy does that for you after 10 minutes of inactivity.**
   1. Since you know everyone in the area this is acceptable
   2. This is not acceptable, you should always log off or lock your computer if you step away
   3. Since you’re only going to be away a short time this is acceptable
   4. Nothing on my computer has value, so this is acceptable

**Answer: b**

1. **You are disposing of old personnel documents that contain sensitive information, what methods of disposal are acceptable?**
   1. Tear the documents into small pieces and dispose of the pieces in multiple trash bins
   2. They are old documents, it is acceptable to just throw them out
   3. Shred the documents using a crosscut shredder
   4. All of the Above

**Answer: c**

1. **Your organization is retiring many computers, many of which processed sensitive information; the plan is to delete all the data from the hard drives and donate them to a charitable institution. Is deleting all data from the hard drives an acceptable media sanitization method?**
   1. Yes
   2. No

**Answer: b**

1. **During a conversation with some colleagues you learn your organization is exchanging sensitive personal information outside your organization via unencrypted email, is this method of transferring sensitive information acceptable?**
   1. Yes, email is an acceptable method of sending sensitive PII unencrypted
   2. No, while email can be used to send sensitive information, it is not acceptable to transfer any sensitive information without encryption.

**Answer: b**

1. **There are many types of sensitive information such as PII, HIPAA, FTI, PCI, etc., and all are governed by State and Federal regulations and policies; regardless the type, all require encryption when moved electronically from one place to another such as email.**
   1. It is stated that the network is private meaning that it is behind a firewall, therefore it is acceptable
   2. Since the network is a private network this is acceptable
   3. A and B
   4. None of the above

**Answer: d**

1. **It’s the end of the day and you are on your way out of the office when you notice that a colleague who has already left for the day has left several files on his desk. You know that these files contain sensitive information, what should your colleague have done with these files before leaving for the day?**
   1. The files should have been secured in an approved storage container
   2. Since the file folders were closed the documents are safe, so leaving them on the desk is okay
   3. Nothing; leaving these closed file folders on the desktop is acceptable
   4. None of the above

**Answer: a**

**Quiz 5 - Be aware of the broad obstacles we face in information security**

1. **Which of the following is an acceptable method of creating a secure password?**
   1. Your children’s or pet’s names
   2. Using substitutions of alphanumeric characters with look-alike numbers or symbols
   3. Using a common name or word from the dictionary
   4. A combination of upper and lowercase letters mixed with numbers and symbols

**Answer: b**

1. **Your computer begins opening programs without your interaction and the mouse is moving on the screen by itself. What should you do?**
   1. Unplug your mouse
   2. Disconnect your computer from the network and call the IT Service Desk
   3. Turn your computer off
   4. Watch for a while to see what is happening

**Answer: b**

1. **Phishing attacks can come from people you know personally**
   1. Yes
   2. No

**Answer: a**

1. **An email comes in from your friend Jill. Jill says she has a new screensaver featuring photos of you and wants you see it. Jill has attached the screensaver file to her email so you can have a look. What is the most appropriate next step?**
   1. Delete the email
   2. Run the screensaver. I want to see those photos!
   3. Save the screensaver for later

**Answer: a**

1. **What is Phishing?**
   1. An encryption method
   2. An online identity theft technique
   3. A well-spent Sunday afternoon on a pier

**Answer: b**

1. **Your supervisor is at home with the flu and calls in to ask you to log into the server using her ID and password because she forgot to run a report. What will you do?**
   1. It sounds like they are in a bind and you’re a team player! Login and run the report.
   2. Deny the request. Remind your supervisor that sharing passwords is bad security practice.
   3. Ignore the request, but get her password first.

**Answer: b**

1. **An email comes in from one of the suppliers at work requesting that you verify the information they have on file. The email contains a link to a website which requests that you enter your username and password in order to proceed. What may be an appropriate next step?**
   1. Call the supplier and enquire whether the email is legitimate before clicking the link
   2. Delete the email immediately
   3. Click the link and enter your username and password
   4. Forward the email to your colleague Bob so he can update his details too

**Answer: a**

**Quiz 6 – What are the threats**

1. **Passwords are strings of characters used to access online services (e.g. your email or social networks profile). However they also help to prevent other people from accessing your personal accounts. Unfortunately, because we use so many services, it is difficult to remember each password that we have. In this situation, what could be a good strategy?**
   1. I save all my different passwords in a file: when I need one, I can easily retrieve it.
   2. I still prefer to use a different password each time.
   3. I use the same password for each service that I use.

**Answer: b**

1. **How many times a week do you read an article on cyber security and hacking? Although both are popular buzzwords they are also of paramount importance in our daily life at work or during our spare time. Generally, who are hackers?**
   1. They are non-threatening computer experts.
   2. They are malicious computer criminals.
   3. Hackers could be both non-threatening computer experts and malicious computer criminals

**Answer: c**

1. **One day you were listening to the evening news while preparing your dinner at home. On the TV show the journalist was interviewing a computer industry expert talking about the importance of regularly updating and patching computer operating systems for security reasons. However you were distracted by cooking and could not understand why he was insisting on that. When thinking about it the day after, you think that patching the operating system…**
   1. Fixes problems and makes the operating system more secure
   2. Allows you to continue using your software without paying.
   3. Improves the working functions of my operating system.

**Answer: a**

**Quiz 7 – Understanding the types of malware Exam**

1. **Malware is software that has a malicious intent to harm users and their devices. A relevant protection in these cases is to have an antivirus software installed. However, even this is not sufficient as the antivirus needs to be constantly updated. What is your perspective about the need for updating the antivirus?**
   1. I Updating of my antivirus should be performed only if I don’ t regularly patch my operating system.
   2. The antivirus update protects my computer from newly created malware.
   3. The antivirus updates ensure the correct performance of my computer.

**Answer: b**

1. **While at work you find that your computer is no longer under your control, what should you do?**
   1. Follow your local security policy procedures
   2. In the absence of official procedures, immediately STOP what you’re doing and contact customer support. If sensitive information is being revealed disconnect the PC from the network, but do not turn it off as critical forensic information may be lost, then contact customer support.
   3. Customer support is working on your computer, wait for them to finish
   4. A and B

**Answer: b**

1. **While at work and surfing the Internet, your computer anti-virus software reports a virus that it is unable to clean, what should you do?**
   1. Immediately close your browser and delete your temporary Internet files
   2. STOP – call customer support
   3. Continue working, the anti-virus has already removed the virus
   4. Delete the infected file, and continue working

**Answer: b**

1. **What is Malware?**
   1. Another name for a virus
   2. Another name for a spyware
   3. Neither A or B
   4. Both A and B

**Answer: c**

1. **You have noticed that your computer is acting erratically and normal tasks (e.g., open a document/application), are taking a little bit longer to perform. So you called a friend of yours who is a computer technician and always helps you when your computer has problems. After a careful inspection he told you that your computer has been infected by a ‘Trojan Horse’. You wonder what a ‘Trojan Horse’ could be?**
   1. It is a computer virus that frequently attack computers.
   2. It is a malicious software that allows other programs to control your computer by misleading users of its true intent.
   3. It is a malfunction of the software that makes it difficult to navigate the Internet.

**Answer: b**

**Quiz 8 – How Malware spreads**

1. **You suspect malware is on your computer, which of the following should you do?**
   1. Stop shopping, banking, and other online activities that involve user names, passwords, or other sensitive information.
   2. Confirm that your security software is active and current. At a minimum, your computer should have anti-virus and anti-spyware software, and a firewall.
   3. Once your security software is up-to-date, run it to scan your computer for viruses and spyware, deleting anything the program identifies as a problem.
   4. Once your security software is up-to-date, run it to scan your computer for viruses and spyware, deleting anything the program identifies as a problem.
   5. All of these

**Answer: e**

1. **You receive an e-mail from your bank telling you there is a problem with your account. The e-mail provides instructions and a link so you can log in to your account and fix the problem. What type of attack could this be?**
   1. Debugging
   2. Browser Hijacking
   3. Social Engineering

**Answer: c**

1. **Which of the following indicate a computer may be infected with malware?**
   1. Slow down, malfunction, or display repeated error messages
   2. Won't shut down or restart
   3. Serve up a lot of pop-up ads, or display them when you're not surfing the web
   4. Display web pages or programs you didn't intend to use, or send emails you didn't write
   5. Any of these

**Answer: e**

1. **What is Spyware?**
   1. Another name of virus
   2. Anti-virus software
   3. Software that monitors or controls your computer use
   4. None of these

**Answer: c**

1. **Which of the following is the best way to protect your computer from external threats?**
   1. Anti-Virus/Spyware software installed with automatic updates
   2. Keeping the computer operating system and all applications patched
   3. Firewall
   4. All of these

**Answer: d**

**Quiz 9 - The Layers of Information Security**

1. **One of your friends has recently been a victim of a social engineering attack since someone has stolen her username and password for accessing her work email. This name, ‘social engineering’ looks quite strange to you as it puts together engineering with social issues. What does social engineering mean in a security context?**
   1. Building systems that are easy to use for society.
   2. It is a form of social deception focused on information gathering, fraud, or system access.
   3. Someone uses social networks for stealing personal data.

**Answer: c**

1. **Access to your building is controlled by your ID badge; arriving at work, a colleague is being courteous and holding the door open for others to enter. Are your colleague’s actions acceptable?**
   1. Yes
   2. No

**Answer: b**

1. **Which of the following should be used to help prevent the theft of your laptop?**
   1. Don't let your mobile device out of your sight, and don’t be showy with your equipment, carrying your gadgets and laptop as inconspicuously as possible is a good idea
   2. Label your property
   3. Use security products; cable locks, lock boxes, or beaconing software
   4. All of these

**Answer: d**

1. **On the road during a business trip you stop to have lunch at a diner, what should you do with your laptop?**
   1. Place it on the passenger seat
   2. Take it with you
   3. Place it in the trunk
   4. Hide it under the seat

**Answer: b**

**Quiz 10 – Password Protection**

1. **Which of the following is the most commonly used (and therefore the weakest) password?**
   1. 123456
   2. Asdf
   3. Iloveyou
   4. Monkey

**Answer: a**

1. **Ideally, what characters should you use in a password to make it strong?**
   1. Letters and numbers only
   2. Mixed Case (Upper and Lower) Characters
   3. Special Characters
   4. All of the above

**Answer: d**

1. **How long should a strong password be?**
   1. 8 Characters
   2. 15 Characters
   3. As long as possible
   4. It doesn’t matter

**Answer: c**

1. **Strong passwords can be difficult to remember, what can you do to avoid forgetting them?**
   1. Use mnemonics (acronyms or phrases that are easy for you to remember)
   2. Develop a password strategy
   3. Use password management software with encryption
   4. All of the above

**Answer: d**

1. **Which of the following should be used when creating passwords?**
   1. Upper and lower case letters
   2. Numbers
   3. Special characters
   4. No dictionary based words or names
   5. Eight or more characters in length
   6. A combination of all the above

**Answer: f**

1. **Which of the following make it acceptable to share your password with another person?**
   1. A coworker needs to do something on your computer when you're out of the office
   2. Your supervisor wants to be able to access any of his or her employees’ computers
   3. Both A and B
   4. Neither A nor B

**Answer: c**

1. **It is considered an acceptable practice to use a group password; a password used by many.**
   1. True
   2. False

**Answer: b**

**Quiz 11 – Malware Protection**

1. **What is Malware?**
   1. Another name for a virus
   2. Another name for spyware
   3. Neither A nor B
   4. Both A and B

**Answer: c**

1. **Which of the following could help you mitigate malwares and viruses from infecting your PC?**
   1. Download software from trusted sources only
   2. Install an antivirus program and a two-way firewall
   3. Always update your PC when prompted for system updates
   4. Install Wireshark to monitor and analyze the traffic of your network

**Answer: c**

1. **Do I currently have an antivirus program installed?**
   1. Yes
   2. No
   3. I do not need one

**Answer: a**

1. **In regards to your antivirus program, have you updated your antivirus program in the last few weeks?**
   1. Yes, I have updated my antivirus program in the last 2 weeks
   2. No, my antivirus program has not been updated in at least 2 weeks.
   3. I am not sure if my antivirus program has been updated in the last 2 weeks.

**Answer: a**

1. **In regards to your antivirus program, are your full scans scheduled to occur automatically on a regular basis or not?**
   1. Yes, full scans are automatically scheduled to occur on a regular basis (daily or weekly).
   2. No, I do not have full scans scheduled at all.
   3. No, full scans are automatically scheduled but occur less often (at least every 2 weeks or longer).

**Answer: a**

**Quiz 12 – Securing your workspace**

1. **A Security investigator dropped 20 "Trojan carrying" USB thumb drives in a Credit Union Parking Lot. According to his report “Of the 20 USB drives we planted, 15 were found by employees, and all had been plugged into company computers” within three days. What should the employees have done with these drives?**
   1. Leave it
   2. Turn it into security
   3. Plug into your computer to seeif there is any information about the rightful owner
   4. Finders, keepers!

**Answer: a**

1. **Which of the following is the best method for reducing the risk of removable media?**
   1. Encryption - encrypt all stored information
   2. Control - implement device and executable control
   3. Education - learn about security risks of removable media and measures to reduce that risk
   4. All of these

**Answer: d**

1. **All removable media should be scanned for viruses before retrieving or storing data on them.**
   1. True
   2. False

**Answer: a**

**Quiz 13 – Physical Security outside the workplace**

1. **You receive an email from a person whose name you recognize, but the domain following the name isn't familiar, what should you do?**
   1. Reply to the email to verify they sent it
   2. Send a new email (not a reply) to the sender using the address from your address book or call the sender to verify they sent it
   3. Delete the email

**Answer: c**

1. **In some situations it may be part of your job to review email from unknown sources, or maybe you just get a lot of email, whichever the reason, the easiest way to quickly and safely move through the list is to use a feature commonly known as ‘previewing’ which allows you to view part or all of the message without actually opening it; this is considered one of the safest methods of viewing email.**
   1. True
   2. False

**Answer: a**

1. **You receive an email from someone you know that has attached files. This person is a colleague that you exchange information with on a routine basis, but the attachments are unusual and have strange file extensions, what should you do?**
   1. Since this is someone you know it's safe to open the attachments
   2. Confirm with the sender via phone call or new email (not a reply), that they sent the email
   3. Forward the email to technical support for verification
   4. Reply to the email requesting confirmation

**Answer: c**

1. **What is Spam?**
   1. SPAM is an anti-virus software solution
   2. SPAM is unsolicited email
   3. SPAM is unsolicited bulk email ("UBE")
   4. SPAM is bulk email

**Answer: c**

1. **You receive an email in your inbox from an unknown address at hotmail.com that claims to be tech support wanting you to install an Internet Explorer update, but the address doesn’t look familiar. The email has a link to download. Upon hovering your mouse over the email, you notice that it isn’t coming from a familiar URL, but looks like the following: (http://www.someserver.loc.ru/ieupdate.exe). Upon trusting the unknown link you get a popup indicating that you need to download and execute 'ieupdate.exe' but your antivirus doesn’t find it malicious. What should you do?**
   1. Open the attachment to install the update
   2. Save the attachment then install the update
   3. Close the download immediately and call tech support
   4. Open the attachment to install the update then call tech support

**Answer: c**

1. **You receive an e-mail from a prominent banker, or so he says. He offers you one million dollars which he got from his uncle, a former well-known politician in a foreign country. He says he needs help sending a vast sum of money, probably millions of dollars, abroad. If you give him your bank account number and let him store the money in your account for a short time, he will give you a million dollars for your trouble.**
   1. Give him your bank account number
   2. Do not give him your bank account number, delete the email
   3. Ask him for more information

**Answer: b**

1. **You receive an email forwarded from a friend with instructions to forward the email again to 10 more friends or you will suffer bad luck for 10 years, what should you do?**
   1. Delete the email
   2. Forward the email
   3. Reply to your friend using a new email and them to stop sending chain email to you
   4. None of the above

**Answer: a**

1. **You receive an email from a reputable local merchant, although you've never done business with them. The email says that you've won a prize, the email instructs that in order to receive the prize you must use the link in the email. What should you do?**
   1. Delete the email
   2. Click on the link
   3. Reply to the email requesting more information
   4. None of these

**Answer: a**

**Quiz 14 – Email Security**

1. **You receive an email from a person whose name you recognize, but the domain following the name isn't familiar, what should you do?**
   1. A. Reply to the email to verify they sent it
   2. B. Send a new email (not a reply) to the sender using the address from your address book or call the sender to verify they sent it
   3. Delete the email
   4. B or C

**Answer: c**

1. **In some situations it may be part of your job to review email from unknown sources, or maybe you just get a lot of email, whichever the reason, the easiest way to quickly and safely move through the list is to use a feature commonly known as ‘previewing’ which allows you to view part or all of the message without actually opening it; this is considered one of the safest methods of viewing email.**
   1. True
   2. False

**Answer: a**

1. **You receive an email from someone you know that has attached files. This person is a colleague that you exchange information with on a routine basis, but the attachments are unusual and have strange file extensions, what should you do?**
   1. Since this is someone you know it's safe to open the attachments
   2. Confirm with the sender via phone call or new email (not a reply), that they sent the email
   3. Forward the email to technical support for verification
   4. Reply to the email requesting confirmation

**Answer: c**

1. **You receive an email in your inbox from an unknown address at hotmail.com that claims to be tech support wanting you to install an Internet Explorer update, but the address doesn’t look familiar. The email has a link to download. Upon hovering your mouse over the email, you notice that it isn’t coming from a familiar URL, but looks like the following: (http://www.someserver.loc.ru/ieupdate.exe). Upon trusting the unknown link you get a popup indicating that you need to download and execute 'ieupdate.exe' but your antivirus doesn’t find it malicious. What should you do?**
   1. Open the attachment to install the update
   2. Save the attachment then install the update
   3. Close the download immediately and call tech support
   4. Open the attachment to install the update then call tech support

**Answer: c**

**Quiz 15 – Social Media Security**

1. **Can I see who has been viewing my Facebook profile?**
   1. Yes, but you need to install an app.
   2. Yes, if you first Like the page for the app.
   3. No, it's impossible.

**Answer: c**

1. **You post a funny picture of a colleague to a social networking site, the next day you learn that the picture is now circulating all over the Internet including your colleagues at work, what can you do?**
   1. Contact customer support of the site to have the pictures removed from the Internet
   2. Contact an attorney you're about to be sued by your friend
   3. There is nothing that can be done
   4. None of these

**Answer: a**

1. **You came across a website that looks exactly like Facebook but it has a different domain which you have never heard of, which of the following is the best course of action that should be taken?**
   1. Hack that website and deface it then post it on Facebook or Twitter.
   2. Launch DDoS (Distributed Denial of Service) attacks into that website with the help of your friends if you can’t hack it in order to take it offline then post it in Facebook or Twitter. #TangoDown!
   3. Do not login into that website and report it as a phishing page to Google Safe Browsing Team – <https://www.google.com/safebrowsing/report_phish/>.
   4. Just ignore that website and login to https://facebook.com instead.

**Answer: c**

1. **Your college best friend has just sent you a chat in Facebook and sent with a link. The link is a shortened URL for example https://goo.gl/wf4V8Z, what should you do?**
   1. Click the link because it shouldn’t be malicious since he/she is your best friend after all. There is nothing to worry about.
   2. Do not click the link and try to check the URL using an online tool that checks where it really takes you.
   3. Contact your local Computer Emergency Response / Readiness Team because it may contain malicious software.d. Install antivirus software, then click the link.
   4. Install antivirus software, then click the link.

**Answer: b**