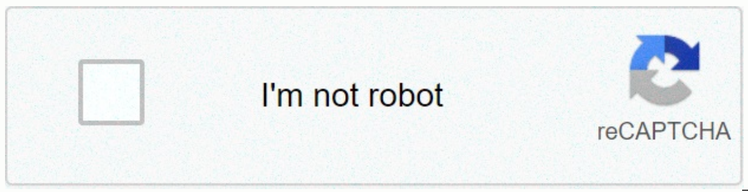

Continue

Cyber awareness challenge 2019 test answers

Product functionality requirements: To meet technical functionality requirements, this awareness product was developed to work with Windows and Mac operating systems (Windows 7 and 10 and macOS 10.13 High Sierra, when properly configured) using internet explorer (IE) 11, Firefox 67, Chrome 75, Microsoft Edge 42, or Safari 12 browsers. Tested Windows-compatible hardware includes surface pro i7 Model 1796. It was also tested for compatibility with Red Hat Enterprise Linux 7.5 using Firefox 52.8.0, as well as Apple iPad Air 2 running iOS 12.3.1 using Safari 12 and Google Chrome 68 browsers and Samsung Galaxy Tab S2 running Android 7 using Google Chrome 64 browser. Using a different operating system or browser is not recommended, since users may not be able to complete the tutorial or save the completion certificate. If you're having trouble starting the tutorial, see the troubleshooting guide. Cybercriminals are working overtime in 2020 with Arkose Labs reporting a 20% increase in fraud and abuse attempts. This is just one reason you need to take steps to protect your organization's sensitive data. If one of your employees received a phishing email, can you say for sure how he or she would respond? This is where the DoD Cyber Awareness Challenge can come in handy. What is the DoD Cyber Awareness Challenge? The Cyber Awareness Challenge, also known as Army Cyber Awareness Training, cyber awareness challenge or DOD cyber challenge for short, is an annual data security training that was created to increase cyber awareness among Department of Defense (DoD) employees. Developed by the United States Defense Information Systems Agency (DISA) this unclassified training is designed to train officers working for branches of the US Department of Defense — which is also known as the DoD Cyber Awareness Challenge — to identify and prevent future cyber attacks. Started with the FBI's Internet Crime Complaint Center (IC3) receiving 23,775 complaints about email compromise (BEC), and that the reporting organizations lost more than $1.7 billion in 2019, you can see that the stakes are high. In fact, the FBI reports that losses from phishing attacks exceeded $3.5 billion in 2019 in 2019. DoD Cyber Awareness Challenge: Who would benefit from this tutorial? Although it is designed for members of the army and the other armed forces branches, anyone can take this cyber awareness challenge. It is available online, it is free for everyone and it is also available from all parts of the world as long as you have a reliable internet connection! That's why we recommended everyone take it. But who would really benefit from this kind of training? Anyone with a computer or who handles all kinds of sensitive information. Companies and organizations can use this cybersecurity challenge as an excellent resource to provide cybersecurity training to their employees. All individuals – especially who value privacy and security, who work with sensitive information, or those working in the IT field, should take this training to protect themselves and their customers from potential cyber attacks. You can complete this training a web awareness challenge on the official DoD Cyber Awareness Challenge 2020 website. Although the lessons focus on securing the country's classified data, the challenge of cybersecurity for non-military users like you and me. In this guide, we will explore the most important lessons in this tutorial for corporate employees and everyone who uses the internet. So, without further delay, let's explore what you can learn from the DoD cyber awareness challenge. The format and main content of the DoD Cyber Awareness Challenge Challenge For Cybersecurity Starts with a dramatic scene showing a piece of future news (from the year 2030), and reveals that due to some cyber attacks, catastrophic events have taken place across the United States. These events took place because some people made bad decisions today (it will want that in 2020). Now, DoD cyber awareness challenge participants show some evidence where people could have made the wrong decisions and asked to make the right choice. There are three main parts and their subsections in the DoD Cyber Awareness Challenge guides: Each section has definitions, vulnerabilities, real-world scenarios, and talks about the types of decisions you should make or avoid to prevent a cyber attack. Computer spills In government, games are a term that refers to information that is leaked from a higher classification or level of protection to a lower one. A spill poses a serious risk to national security. Gaming occurs when someone accidentally or intentionally makes unauthorized data disclosure, data change, or engages in espionage, resulting in loss or degradation of resources or capabilities. Sensitive information For any type of business or organization that handles sensitive information, it is essential that you do everything you can to protect this information— both for the sake of customers, as well as to remain compliant with regulatory data protection laws and requirements. Some of these regulations include: But what is considered sensitive information? Sensitive information includes: Official Use Only (RUO),Controlled Unclassified Information (CUI),Controlled Technical Information (CTI),Personal Identifiable Information (PII),Protected Health Information (PHI),Financial Information, Personal Information or Payroll Information and Proprietary Data. This type of sensitive information must be protected because the leak can compromise public missions or interests. An example of such sensitive information includes data or information provided by a confidential source (person, commercial or foreign government) on the condition that it would not be released. For businesses and health organisations, examples These types of information include: Employee or customer names, addresses, phone numbers, etc., Financial records and account information, User credentials and passwords, Patient records and health-related information, and Medical or insurance information. Malicious code Malicious code can be disseminted by downloading corrupted email attachments and files or visiting infected websites. Malicious code includes viruses, Trojan horses, worms, macros and scripts. They can damage or compromise digital files, delete your hard drive and/or allow hackers to access your PC or phone from a remote location. Important lessons for companies and individuals from the DoD Cyber Awareness Challenge Methods of cybercrimes are going to be the same, whether the goal is government, private companies or members of the public. That's why there are many important lessons this cybersecurity challenge contains that can help corporate employees and individuals prevent such attacks. Here we have written a summary of training of cybersecurity challenges, covering the main takeaway lessons. Please note that we have only included hand-picked lessons that we consider beneficial to a general audience. But it does not have all the teachings of the course. To access all this, you need to complete the DoD Cyber Awareness Challenge yourself! Protection against malicious code malicious code is a term that describes the code used in electronic forms, scripts, and software that aims to cause damage in one way or another. Here are some useful tips to help your employees avoid the risks associated with downloading and installing malicious code: Scan all external files before uploading them to your computer. Cannot access site links, buttons, and/or graphics in a suspected email or pop-up window generated by an email message. If you suspect that email is harmful, or if an unknown/unauthorized sender requests personal/sensitive information, contact the Security Contact Point (POC) or Support for assistance. For your personal and office devices (laptop, PC, mobile, etc.), research any program and its vulnerabilities before downloading it. View email in plain text, and don't show an email in the preview pane. Look for digital signatures if your organization uses an email signing certificate (highly recommended). Digitally signed emails are considered more secure. Best practices for protecting sensitive information When you trust your employees to handle your customers' confidential information, they need to be aware of the sensitivity of your data and how to protect it. A single act of negligence can be disastrous. Here are some big takeaways from the cyber awareness challenge that you can use to train your staff. When faxing sensitive information, make sure that the recipient is in the receiving page. Contact the recipient to confirm the reception. The most commonly reported cause of PII fracture failure to encrypt emails containing PII. So always use encryption when PII, PHI or other sensitive information. Also digitally signed emails when it is possible to provide authentication and to ensure information integrity. Avoid storing sensitive information in shared folders or shared applications (e.g. SharePoint, Google Docs, etc.). Never use personal email accounts for transferring PII and PHI. Store sensitive data only on authorized information systems. Do not send, store, or process confidential information about unauthorised systems. Follow your organization's guidelines for storing or disposing of sensitive information. Mobile devices may be hacked or infected with malware. Therefore, always use mobile devices that are approved by your organization and follow your organization's guidelines for using mobile computing devices and encryption while working with PII or PHI. Prevention against insider threats Incidents related to insider threats are up 47% since 2018, according to data from the Ponemon Institute and ObserveIT. The term insider threat refers to a situation where employees themselves (intentionally or inadvertently) leak the data or carry out the cybercrime against the organization. You can't rule out the possibility of insider threats because employees have tons of information readily available to them at their fingertips. So, as an employer, you need to keep an eye on your employees' activities and also train your employees to recognize the potential threat that may exist among them. We're not saying all your employees are insider threats. But if someone goes through difficult life situations or experiences persistent interpersonal difficulties, their emotional instability can make them a potential candidate to become one. Follow them and consider whether they show unusual or about behavior, such as: Display hostile, vindictive or criminal behavior, orPlay an unusual or excessive interest in sensitive information or Inaugurate unexplained or sudden prosperity when purchasing high-value elements/living beyond one's means or Attempting to access and/or remove sensitive information without the need to know instead of providing the benefit of the doubt, reporting suspicious activity or behavior in accordance with the agency's insider threat. Of course, there are several steps you can take to prevent or limit the impact of insider threats: Perform risk assessments for your entire organization. Create and enforce a data usage policy. Implement the principle of least privilege to restrict employee access to only necessary systems. Regularly review access lists and remove access immediately for employees who quit or are fired. Use a security information and an event system (SIEM) to monitor employee actions and the information they access. Workplace physical safety practices There are many reasons why physical safety is so important to organizations – your colleague can be an insider threat, or some walk-ins or can spy, eavesdrop or look for a to steal important data from your files or computer. These events occur not only on military installations, but also in the organizations. So you need to be vigilant about safety in your workplace as well. This means: Do not talk about work / customers / company guidelines for marketing, technology, etc. outside the workspace. You may inadvertently leak any confidential information that does not have to go out. Even inside a closed working environment, be careful when discussing sensitive information, such as PII or PHI, as people without the need to know may be present around you. Note that people are eavesdropping when you retrieve messages from smartphones or other media. Know and follow your organization's guidelines for accessing the building, secure workspace and respond to emergencies. Always lock the office cabinets and drawers if they have files/papers containing sensitive information. Best practices for portable devices and removable media portable devices and removable media pose a major security threat to both businesses and government organizations. They are easy to use and practical. However, portable devices can also carry malware from one device to another without the user knowing. So if you connect an infected device to a new machine, it can install the malware on the new device. These media types include flash media, such as flash drives, flash

drives and flash drives, external hard drives, optical discs, and external music players such as iPods. So, what can you do to protect your organization? Use only removable media to store work-related data when it is operationally required, owned by your organization, and approved by the appropriate authority in accordance with the guidelines. Encrypt data correctly when you save it to a removable media device. Do not use any personally owned/non-organizational removable media to store your organization's data. As a best practice, you can tag all removable media, especially if they contain PII, or PHI or sensitive data. Avoid inserting removable media with unknown content into your computer. Follow your organization's guidelines for cleaning, cleaning, discarding, and destroying removable media best practices for laptops and mobile devices The laptop and mobile devices must have stored as many stored credentials for automatic sign-in, personal and professional data, and media files. If your organization has given you a laptop or mobile for professional use, it could be a virtual gold mine for attackers. Only by hacking or stealing such devices can cybercriminals carry out dangerous attacks. That's why it's a crucial step to give your phone and laptop a close. Consider screen protection if you're using a portable or mobile device to do office work in public places. Turn off your device if you're not going to use it in the near future. Turn on automatic screen locking after a period of inactivity. all sensitive data on laptops/mobile. Always maintain visual or physical control over portable/mobile devices, especially when you go through airport security checkpoints. Use public or free Wi-Fi only with your organization's approved VPN. If your device is lost or stolen, you must immediately report the loss to your security INTEREST OR your organization's technology department. Home Computer Security Tips People typically don't store organization-related information on your home computer/computer. However, such personal computers contain automatic login facilities to email addresses, social media, applications, financial institutions' websites, etc. Therefore, employees need to be aware of how to protect their home computers as well. Note: In the cybersecurity awareness challenge, these tips are taken from the National Security Agency (NSA)'s PDF Best Practices for Keeping Your Home Network Secure. Always use strong passwords for your home computer. Create separate accounts for each user and have them create their own passwords using a strong password creation method. Install all system security updates, updates, and keep your defenses, such as antivirus software, spyware, and firewall up to date. Regularly scan for viruses. Change the default login ID and password for operating systems and applications. Back up files regularly and securely save your files. Beware of sudden flashing pop-ups warning that your computer is infected with a virus; This may indicate a malicious code attack. General online behavior safety tips Outside the workplace Although employers can't necessarily control what employees do in their personal time, they can teach them about the dangers of social media and other online platforms. The DoD Cyber Awareness Challenge has a section that provides guidance on the best practices while browsing the web. Here are some important takeaways from this section of the DoD cyber awareness challenge training: Be aware of the information you post online about yourself and your family. It can be used to guess your passwords, perform doxxing attacks, send spear/whale phishing emails or for identity theft. Create strong passwords and choose two-factor authentication (2FA) or multi-factor authentication (MFA), if available. Beware of links to games, quizzes and other applications available through social networking services. They may contain malicious codes or manipulate you into sharing your login information or other sensitive information. Don't post confidential information about your organization, colleagues, or customers on social networking sites (no matter what privacy settings you've set on your account). A final word on the DoD Cyber Awareness Challenge Cybercriminals uses innovative and sophisticated ways to carry out cyber attacks today. People fall for such malicious tricks and lose billions of dollars every year. That is why training online awareness is a must for everyone, especially for corporate employees and people working in technology. When companies fall victim to a cyber attack due to negligence of an employee or insider threats, they lose not only sensitive data, but also their reputation and suffer from financial loss in legal battles. As such, the DoD Cyber Awareness Challenge is an excellent resource for organizations to train their employees, make them vigilant against various types of cyber crimes, and let them know the best protection techniques. The challenge of cybersecurity is a highly recommended training for everyone to improve the security position of any organization regardless of size. Size.