# TEXT STRUCTURE SAMPLE (WEEK 1)

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Course | Author | Activity | Week | Title | description | keywords | Document |
| ADVANCED CYBERSECURITY TRAINING FOR TEACHERS (ACTT) | Teachers Future | 1A | 1 | Identifying Phishing Emails | Phishing emails are the most common form of online fraud where attackers try to acquire sensitive data from users. In this activity, we are going to identify and learn the features of a phishing email. (pg.1-2) | Phishing, Email, cyber security,fraud,sensitive data, attackers | Activity 1A Identifying Phishing Emails.pdf |
| ADVANCED CYBERSECURITY TRAINING FOR TEACHERS (ACTT) | Teachers Future | 1B | 1 | Blocking Websites on a Personal Computer Using Linux | A firewall filters incoming and outgoing traffic in the network and utilizes rules that either block or allow the connection. It can be a software application or hardware device. In this activity, we are going to use a Linux terminal to block a personal device from accessing the Facebook website. From the image below you can see that we have successfully accessed the Facebook website. Confirm you can view the Facebook website by going to facebook.com on your browser. (pg.1-3) | Block website, Linux, Facebook, Linux terminal, cybersecurity, fakebook.com, Show Applications, 127.0.0.1, www.facebook.com, Save | Activity 1B Blocking Websites on a Personal Computer Using Linux.pdf |
| ADVANCED CYBERSECURITY TRAINING FOR TEACHERS (ACTT) | Teachers Future | 1B | 1 | Unblocking Facebook Website | To unblock Facebook on Linux, follow these steps. (pg.4-5) | unblock website, Linux, Facebook, password, cybersecurity, Show Applications, Sudo , gedit /etc/hosts, terminal, 127.0.0.1 www.facebook.com,Save, screenshot | Activity 1B Blocking Websites on a Personal Computer Using Linux.pdf |
| ADVANCED CYBERSECURITY TRAINING FOR TEACHERS (ACTT) | Teachers Future | 1B | 1 | Blocking Websites on a Personal Computer Using;  MacOS | A firewall filters incoming and outgoing traffic in the network and utilizes rules that either block or allow  the connection. It can be a software application or hardware device. In this activity, we are going to use a  MacBook to block a personal device from accessing the Facebook website.  From the image below you can see that we have successfully accessed the Facebook website. Confirm you  can view the Facebook website by going to facebook.com on your browser. (pg.1-4) | Facebook website, MacBook, Launchpad, terminal, utilities, search text field, click, Sudo, nano, -e /etc/hosts, e text edit mode, password, e 127.0.0.1, www.facebook.com, local IP address, laptop, flush the cache, dscacheutil –flushcache, web, browser | Activity 1B Blocking Websites on a Personal Computer Using MacOS.pdf |
| ADVANCED CYBERSECURITY TRAINING FOR TEACHERS (ACTT) | Teachers Future | 1B | 1 | Unblocking Facebook Website MacBook. | To unblock Facebook on a Mac OS, follow the following steps. (pg.4-7) | Launchpad icon, applications, Utilities, Terminal, Sudo, nano, -e /etc/hosts, Delete, 127.0.0.1 [www.facebook.com](http://www.facebook.com), cache, flush, dscacheutil –flushcache, Ctrl + X, editor, unblock | Activity 1B Blocking Websites on a Personal Computer Using MacOS.pdf |
| ADVANCED CYBERSECURITY TRAINING FOR TEACHERS (ACTT) | Teachers Future | 1B | 1 | Blocking Websites on a Personal Computer Using Windows Firewall. | A firewall filters incoming and outgoing traffic in the network and utilizes rules that either block or allow the connection. It can be a software application or hardware device. In this activity, we are going to use Windows Defender Firewall application to block a personal device from accessing the Facebook website. A firewall filters incoming and outgoing traffic in the network and utilizes rules that either block or allow the connection. It can be a software application or hardware device. In this activity, we are going to use Windows Defender Firewall application to block a personal device from accessing the Facebook website. (pg.1-10) | Firewall, filter,network, Windows Defender, Facebook, fakebook.com o, Control Panel, open, System and Security, Advanced Settings, k Inbound Rules, custom,next, All Programs, IP address, command prompt, nslookup fakebook.com, Which remote IP addresses does this rule apply to? Block the Connection, finish, Outbound Rules, next, finish | Activity 1B Blocking Websites on a Personal Computer Using Windows Firewall.pdf |
| ADVANCED CYBERSECURITY TRAINING FOR TEACHERS (ACTT) | Teachers Future | 1B | 1 | Unblocking Facebook website | Navigate to Windows Defender Firewall ...(pg.10) | No Facebook Access, delete, Outbound Rules | Activity 1B Blocking, Websites on a Personal Computer Using Windows Firewall.pdf |
| ADVANCED CYBERSECURITY TRAINING FOR TEACHERS (ACTT) | Teachers Future |  | 1 | Advanced Cyber Attacks Resources | Attack Vectors, Wireless and Mobile Device Attacks, Application and Web Attacks, Internal Threats (pg. 1-2) | Securing, WhatsApp, account, Vishing  Smishing  Insecure, Wi-Fi Network,  Windows, Security, Public, Wi-Fi, identify, Classic Phishing, Ransomware  , Zero-day exploit  ,Malvertising  Case Studies  Zoom Bombing  Mount Kenya University Data Leak, Break Network  Hacks School ,Data Leak, Internal Threats, Chicago, Public School,  Highschool Kobe  Korea Credit, Bureaus,  Microsoft Corporation, database.  Henry Park Primary School,  Marine | Week 1 Advanced Cyber Attacks Resources .pdf |
| ADVANCED CYBERSECURITY TRAINING FOR TEACHERS (ACTT) | Teachers Future |  | 1 | Attack surface and attack | (pg.3) | Exploit, device, network, attacker, unauthorized access | Week 1 Attack Vector.pptx |
| ADVANCED CYBERSECURITY TRAINING FOR TEACHERS (ACTT) | Teachers Future |  | 1 | Common types of attack vectors | (pg.4) | Compromised, credentials, Weak, stolen credentials, Malicious ,insiders, Misconfiguration,Vulnerabilities,Malware | Week 1 Attack Vector.pptx |
| ADVANCED CYBERSECURITY TRAINING FOR TEACHERS (ACTT) | Teachers Future |  | 1 | An attack vector can be classified as either | (pg.5) | Passive, active | Week 1 Attack Vector.pptx |
| ADVANCED CYBERSECURITY TRAINING FOR TEACHERS (ACTT) | Teachers Future |  | 1 | Active attack vector | (pg.6) | Integrity, system,malware,exploit, misleading message, sender | Week 1 Attack Vector.pptx |
| ADVANCED CYBERSECURITY TRAINING FOR TEACHERS (ACTT) | Teachers Future |  | 1 | Active attacks are in the form of | (pg.7) | Interruption,modification,fabrication,network,capture,deny,system | Week 1 Attack Vector.pptx |
| ADVANCED CYBERSECURITY TRAINING FOR TEACHERS (ACTT) | Teachers Future |  | 1 | Types of Active Attacks | (pg.8-11) | Masquerade,data,theft, impersonates legitimate, unauthorized, access, network, resources, Repudiation, eavesdrops, secure network communication,cyber-attack,traffic | Week 1 Attack Vector.pptx |
| ADVANCED CYBERSECURITY TRAINING FOR TEACHERS (ACTT) | Teachers Future |  | 1 | Passive attack vector | (pg.12) | threat , data confidentiality, system resources, modifying contents | Week 1 Attack Vector.pptx |
| ADVANCED CYBERSECURITY TRAINING FOR TEACHERS (ACTT) | Teachers Future |  | 1 | Types of Passive Attacks | (pg.13-17) | Message Release, transmission, telephonic conversation, ,e-mail,location, Dumpster diving, shred documents, format devices,trash bin, Baiting, branded flash disks, private information, Piggybacking / Tailgating, authorized person | Week 1 Attack Vector.pptx |
| ADVANCED CYBERSECURITY TRAINING FOR TEACHERS (ACTT) | Teachers Future |  | 1 | Similarities between active and passive attack vectors | (pg.18) | Pretexting, social engineering, fictional backstory | Week 1 Attack Vector.pptx |
| ADVANCED CYBERSECURITY TRAINING FOR TEACHERS (ACTT) | Teachers Future |  | 1 | Difference between Active and Passive attack vector | (pg.19) | social engineering, malware or phishing,tools,exploit, steal sensitive, data, install, malicious ,code, computer or network | Week 1 Attack Vector.pptx |
| ADVANCED CYBERSECURITY TRAINING FOR TEACHERS (ACTT) | Teachers Future |  | 1 | Protection against attack vectors | (pg.20) | Principle of Least Privilege, cybersecurity, tools, firewalls , secure communications, Encrypt, sensitive, information, ,data, in-transit, two-factor authentication,minimize,maximize,breach, truste,monitor | Week 1 Attack Vector.pptx |
| ADVANCED CYBERSECURITY TRAINING FOR TEACHERS (ACTT) | Teachers Future |  | 1 | Attack Vectors Writeup | Before tackling attack vectors, we must first understand the term attack surface. Attack surface and  attack vectors are easily mistaken to mean the same. On the contrary, they mean different. An attack  surface is the number of feasible ways an attacker can exploit to get into a device or network.  What is an attack vector? An attack vector is simply the method an attacker uses to compromise a  device or network and gain unauthorized access. (pg.1-8) | malware, exploiting, vulnerabilities, man-in-the-middle ,ransomware, Repudiation,rplay,denial of service, Passive attack vector, Dumpster diving, SMS, e-mails ,web advert, Baiting, branded flash disks, private information, Piggybacking / Tailgating, authorized person, minimal access rights,vpn, firewalls, password managers | Week 1 Attack Vectors Writeup.pdf |
| ADVANCED CYBERSECURITY TRAINING FOR TEACHERS (ACTT) | Teachers Future |  |  | Attack Vector Transcript | Hello participant, welcome to the first week of the ACTT course. I am your instructor, Murrey Eddah.  This  week will focus on advanced cyber-attacks and build-up on the knowledge you have on cyber-attacks. (pg.1-4) | phishing email, redirecting link, branded corporate branded flash disk, piggybacking ,tailgating , unauthorized person, Pretexting, social engineering, financial transaction, computer, network, steals information, Training of staff and students, Apply ,Principle of Least Privilege, firewalls, password  managers , VPNs , secure communications, Patch operating system, update device software to,latest version, Encrypt sensitive information -data at rest, in-transit and in- processing, Monitor data ,network access , users devices , unmask insider risk and Use two-factor  authentication, cybersecurity | Week 1 Attack Vector Transcript.pdf |
| ADVANCED CYBERSECURITY TRAINING FOR TEACHERS (ACTT) | Teachers Future |  | 1 | Internal Threats | Humans are the weakest link when it comes to the implementation of cybersecurity.  An internal threat refers to the risk emerging inside a company, government agency, or institution and affects the computer system. (pg.3) | government agency, institution, computer system | Week 1 Internal Threats.pptx |
| ADVANCED CYBERSECURITY TRAINING FOR TEACHERS (ACTT) | Teachers Future |  | 1 | Internal threats can be caused by | (pg.4) | Employee sabotage, theft ,data ,physical equipment, Unauthorized access, secure areas , administration, computer equipment ,fire, flooding, power loss or terrorism, Accidental loss , disclosure , data | Week 1 Internal Threats.pptx |
| ADVANCED CYBERSECURITY TRAINING FOR TEACHERS (ACTT) | Teachers Future |  | 1 | Insider Threat | (pg.5) | exploit system , cause damage, employee , contractor, sensitive information , privileged accounts, orchestrating damage, threat , company | Week 1 Internal Threats.pptx |
| ADVANCED CYBERSECURITY TRAINING FOR TEACHERS (ACTT) | Teachers Future |  | 1 | Types of insider threats | (pg.6-7) | Ponemon Institute, phishing schemes, Malicious insider/ turn cloak, steal information, Careless insider,pawn, mistake maker, mole, imposter | Week 1 Internal Threats.pptx |
| ADVANCED CYBERSECURITY TRAINING FOR TEACHERS (ACTT) | Teachers Future |  | 1 | Common Causes of insider threats | (pg.8) | Disgruntled, employees, steal ,leak ,data, online, Negligence , awareness | Week 1 Internal Threats.pptx |
| ADVANCED CYBERSECURITY TRAINING FOR TEACHERS (ACTT) | Teachers Future |  | 1 | Indicators of a Malicious Insider Threat | (pg.9) | Digital ,Warning ,Signs  Behavioural | Week 1 Internal Threats.pptx |
| ADVANCED CYBERSECURITY TRAINING FOR TEACHERS (ACTT) | Teachers Future |  | 1 | Digital Warning Signs | (pg.10) | Data,sensitive,profile,job,resources,usb,drive,email,hoarding,network | Week 1 Internal Threats.pptx |
| ADVANCED CYBERSECURITY TRAINING FOR TEACHERS (ACTT) | Teachers Future |  | 1 | Behavioural Warning Signs | (pg.11) | Violation,bypass,security | Week 1 Internal Threats.pptx |
| ADVANCED CYBERSECURITY TRAINING FOR TEACHERS (ACTT) | Teachers Future |  | 1 | Fighting Internal Threats | (pg.12-15) | school , institution deter attacks loss, detect attacks, secure state, background checks,employee, Microsoft Network Monitor,security,student,staff, behavioural activities,monitor, assets, vulnerabilities ,phishing,email | Week 1 Internal Threats.pptx |
| ADVANCED CYBERSECURITY TRAINING FOR TEACHERS (ACTT) | Teachers Future |  | 1 | Case Studies on Insider Threat | (pg.16) | Microsoft Corporation database, Microsoft Excel | Week 1 Internal Threats.pptx |
| ADVANCED CYBERSECURITY TRAINING FOR TEACHERS (ACTT) | Teachers Future |  | 1 | INTERNAL THREATS | Hello participant, welcome to the last topic of week one. I am your instructor, Murrey Eddah. In this  video,  we will learn about internal threats, how to identify them and their consequences.  An internal threat refers to the risk emerging inside a company, government agency, or institution and  affects the computer system. (pg.1-4) | Murrey Eddah, risk emerging i company, government agency, or institution, Employee sabotage, theft data, Unauthorized access, Damage computer equipment  fire, flooding, power loss , terrorism, institution’s secrets, case studies , cyber incidents, attack vectors , phishing email, USB drives , floppy disks, Ponemon Institute,law suit,school,data | Week 1 Internal Threats Transcript.pdf |
| ADVANCED CYBERSECURITY TRAINING FOR TEACHERS (ACTT) | Teachers Future |  | 1 | Internal Threats Writeup | Humans are the weakest link when it comes to the implementation of cybersecurity. An internal threat  refers to the risk emerging inside a company, government agency, or institution and affects the  computer system. | company, government agency, institution,data,theft,equipment,terrorism, fire, flooding, power loss, Malicious insider, turn cloak, Careless insider,pawn, mistake maker, mole, imposter, Negligence , lack of awareness, sensitive data,hoarding, Behavioural Warning Signs, names, employee ID numbers, phone numbers, addresses, birth dates, criminal histories,, health conditions, records, Microsoft Corporation database, Korea Credit Bureaus, Henry Park Primary School, Microsoft Excel file. | Week 1 Internal Threats Writeup.pdf |
| ADVANCED CYBERSECURITY TRAINING FOR TEACHERS (ACTT) | Teachers Future |  | 1 | Software Application and Web Attacks | Threat actors exploit an application installed in a laptop or phone by leveraging the vulnerabilities  present. This can result in unauthorized access to privileged information such as a physical address,  teacher profiles and student profiles. The following online learning platforms can be affected by a  software application attack: Learning Management Systems (LMS), Student Management Systems (SMS)  and video conferencing (Zoom, Microsoft Teams, Google Meets, Webex). | Learning Management Systems (LMS), Student Management Systems,SMS,video,video conferencing, Zoom, Microsoft Teams, Google Meets, Webex. | Week 1 Software Application and Web Attacks Article.pdf |
| ADVANCED CYBERSECURITY TRAINING FOR TEACHERS (ACTT) | Teachers Future |  | 1 | Common Software Application Attacks | Threat actors exploit an application installed in a laptop or phone by leveraging the vulnerabilities  present. This can result in unauthorized access to privileged information such as a physical address,  teacher profiles and student profiles. The following online learning platforms can be affected by a  software application attack: Learning Management Systems (LMS), Student Management Systems (SMS)  and video conferencing (Zoom, Microsoft Teams, Google Meets, Webex). (pg.1-4) | Ransomware, Phishing, Brute force attack, Zero-day attack | Week 1 Software Application and Web Attacks Article.pdf |
| ADVANCED CYBERSECURITY TRAINING FOR TEACHERS (ACTT) | Teachers Future |  | 1 | Common Web Attacks | Humans are considered the weakest link in cybersecurity. Most users are confident that information  stored in a trusted website is safe and will be kept private. However, a threat actor can identify  loopholes in the website, gain access and read the user’s confidential information. A web attack can  affect a school’s website, student and staff portal. (pg.4-5) | Watering Hole Attack, Drive-by Download Attack, Malvertising, Website Spoofing, Insecure connections | Week 1 Software Application and Web Attacks Article.pdf |
| ADVANCED CYBERSECURITY TRAINING FOR TEACHERS (ACTT) | Teachers Future |  | 1 | Wireless Attacks | Wireless networks have made life easier, especially during the Covid-19 pandemic, whereby schools  closed, and learning and teaching from home became the new norm. However, wireless networks are  susceptible to attacks that can cause great harm to a device and the user.  A wireless attack is a malicious action against wireless networks or wireless system information. An  example is a rogue access point.(pg.1) |  | Week 1 Wireless and Mobile Device Attacks Article.pdf |
| ADVANCED CYBERSECURITY TRAINING FOR TEACHERS (ACTT) | Teachers Future |  |  | Common Wireless Vulnerabilities | A vulnerability is a weakness that can be exploited by a hacker to compromise a device or network.(pg.1-2) | Default SSIDs, Passwords, Access Point Location, Wired Equivalent Privacy (WEP) Protocol, Access 2 (WPA2) or Wi-Fi Protected Access 3 (WPA3) en, frequencies, 2.5 GHz and 5 GHz, signal strength, wi-fi | Week 1 Wireless and Mobile Device Attacks Article.pdf |
| ADVANCED CYBERSECURITY TRAINING FOR TEACHERS (ACTT) | Teachers Future |  | 1 | Types of Wireless Attacks | (pg.2-5) | War-driving, Jamming, Rogue Access Points, Evil Twin Access Points, Packet capturing and sniffing, War shipping | Week 1 Wireless and Mobile Device Attacks Article.pdf |
| ADVANCED CYBERSECURITY TRAINING FOR TEACHERS (ACTT) | Teachers Future |  | 1 | Wireless Attacks Scenarios | (pg.6) | Russian agents, hack victims remotely, surveillance machines, tracking locations, shut down, phone lines, internet | Week 1 Wireless and Mobile Device Attacks Article.pdf |
| ADVANCED CYBERSECURITY TRAINING FOR TEACHERS (ACTT) |  |  | 1 | Wireless Attacks Countermeasure |  | untrusted networks ,vpn, t software update, strong unique passwords, Remote Access,firewall,device | Week 1 Wireless and Mobile Device Attacks Article.pdf |
| ADVANCED CYBERSECURITY TRAINING FOR TEACHERS (ACTT) | Teachers Future |  | 1 | Mobile Device Attacks | What do your mobile devices know about you? | smartphone, access passwords, social security information, files, passwords, messages, emails, addresses, location information, web history and banking information. impersonate, stealing identity, commit crime | Week 1 Wireless and Mobile Device Attacks Article.pdf |
| ADVANCED CYBERSECURITY TRAINING FOR TEACHERS (ACTT) | Teachers Future |  | 1 | What are mobile device attacks? | A mobile device attack is an exploit targeting handheld or portable communication devices such as a cell  phone, smartwatch, Bluetooth headset, laptops and tablets. 1 Most educators and learners use  smartphones and laptops during online classes. (pg.7) | devices cell phone, smartwatch, Bluetooth headset, laptops, tablets | Week 1 Wireless and Mobile Device Attacks Article.pdf |
| ADVANCED CYBERSECURITY TRAINING FOR TEACHERS (ACTT) | Teachers Future |  | 1 | Types of mobile threats | App-based, Web-based, Network-based, Physical(pg.7-8) | play store, App-Store, exploit, fraudulent intentions, malicious, Wi-Fi , Bluetooth technologies, Windows, Android or iOS | Week 1 Wireless and Mobile Device Attacks Article.pdf |
| ADVANCED CYBERSECURITY TRAINING FOR TEACHERS (ACTT) | Teachers Future |  | 1 | Effects of a mobile device attack | (pg.8) | SMS texts, capture call logs, emails, GPS location, phone | Week 1 Wireless and Mobile Device Attacks Article.pdf |
| ADVANCED CYBERSECURITY TRAINING FOR TEACHERS (ACTT) | Teachers Future |  | 1 | Types of mobile device attacks | (pg.8-13) | Malware, Adware, Browser exploit, Trojan, Spyware, Phishing, Clone phishing, Email phishing, Smishing, Vishing, Bluetooth Exploits, Bluejacking, Bluebugging, Bluesnarfing, Blue Borne | Week 1 Wireless and Mobile Device Attacks Article.pdf |
| ADVANCED CYBERSECURITY TRAINING FOR TEACHERS (ACTT) | Teachers Future |  | 1 | How to keep your mobile device secure? | (pg.14) | phone, lock, secure application, encrypts communication, Signal, WhatsApp, Chat Secure, secure complex patterns, passwords, fingerprint, face recognition, encryption tools, Zeal Crypt, Crypto, advert blocking application, AdBlock Plus, Ad-Blocker and Ad Guard, anti-virus software, two-step verification PIN | Week 1 Wireless and Mobile Device Attacks Article.pdf |
| ADVANCED CYBERSECURITY TRAINING FOR TEACHERS (ACTT) | Teachers Future |  | 1 | Additional Reading Material on WhatsApp Security | (pg.14) | Secure, WhatsApp account,chat | Week 1 Wireless and Mobile Device Attacks Article.pdf |