1

Consult with stakeholders

1. You are now required to interview a **minimum of 6 people in the work area. Record your interview with each of the 6 people. This may be done as a group consultation however each person will need to complete the survey form.**

   It is important to obtain information from people working in a range of different disciplines within the organisation (e.g.; finance, administration, legal etc).

2. You will now collate and review the information you have obtained and provide a report for management about the findings. Your report will need to use clear, specific and industry-related terminology relating to cyber security

Cyber Security Finding Review Report
Overview of findings from information gathered from work area - including current trends identified in the work areas cybersecurity awareness and workplace practice of the staff.
As we all know, cybersecurity is a process designed to protect networks and devices from external compromise. Companies often hire cybersecurity professionals to protect their sensitive information, maintain employee productivity, and increase customer confidence in their products and services. The following is the overview of findings from information gathered including current trends identified in the work areas cybersecurity awareness and workplace practice of the staff 1.**Denial of Service, or DOS** Where a hacker consumes all of a server's resources, so there's nothing for legitimate users to access 2.**Man in the Middle Attack** Hackers are placed between the victim's machine and the router to sniff out packets 3.**Phishing** Where a hacker sends a seemingly legitimate-looking email asking users to disclose personal information 4.**Malware** Where victims are hit with a worm or virus that renders their devices useless

Examples where current practice is complying with organisational policies and procedures: □ Using strong passwords & use a password management tool □ Using two-factor or multi-factor authentication. □ Learning about phishing scams – be very suspicious of emails, phone calls, and flyer		
3 Cybersecurity work practices or awareness that do not align with the organisation's policies and procedures or best practice (Potential threats)		Potential impact on the company
1.	Use multifactor identification	Without multi-factor authentication (MFA), cybercriminals can much more easily gain access to employee's accounts.
2.	Enforcing safe password practices	The stronger your password, the more protected your computer will be from hackers and malicious software. Employees should maintain strong passwords for all accounts on their computers.
3.	Organizing employees' training on cyber security	When employees don't optimal safety training, They couldn't have been more likely Monitor potential threats and Report all incoming events.
Suggested ways to improve cybersecurity awareness for each of the 3 potential threats identified		
1.	Using anti-virus protection & firewall	
2.	Learning about phishing scams – be very suspicious of emails, phone calls, and flyers.	
3.	Using anti-virus protection & firewall	

Submit your answers electronically via the Learning Management System.

- **e.g. AB_BSBXCS402_Task 3 Cyber Security Finding Review Report _v1.0**

Part B Create Cybersecurity awareness program about 2 cyber security matters.

Based on your report you are required to develop a cybersecurity awareness program for colleagues that support and promote cybersecurity practice and awareness in relation to **2 different cyber security matters.**

CYBERSECURITY AWARENESS PROGRAM	
Trainer Name:	
Planned training date:	
Planned training time from/to:	11am-12am
Cyber Security Matter 1: Denial of Service(DOS) attack	
Cyber Security Matter 2: Phishing attack	
Objectives of the training to meet organisation-wide practice: The main goal of the training is to officially educate employees about the various cyber threats that exist, how to identify them, and the steps that need to be taken to ensure their own safety and the safety of the company. 1.Train on how to use an anti-virus program 2.Identification of phishing emails	
Skills to be developed: 1. Keep up with cybersecurity compliance regulations 2. Prevent employees from falling for phishing scams	**Knowledge to be developed:** 1.ncorporate cybersecurity into the company culture 2.Reduce the likelihood of a successful breach

Training method/s:

Demonstration

Explanation

Showing videos

Providing examples

Research and discussion

Simulated training method (list the technology platforms to assist with promoting cyber security) :

The following security platforms will provide well-defined and flexible response and mitigation options Threats, including automatic and manual variants.

Examples of penetration testing tools and frameworks include malware protection, Metasploit, Kali Linux,Zoom meetings, Windows security firewalls, etc.

Training location:Trainings Hall

Training activities		**Resources required**
1.	Test their knowledge	Workplace policies and procedures, Anti virus program
2.	Ask participants to run the program themselves Workplace policies and procedures, Anti virus	Workplace policies and procedures, Anti virus program
3.	Show how to run the anti-virus program	Anti-virus program

4.	Discuss the video and presentation	Video software, workplace policies and procedures
5.	Present the PTT and show the Video	Computer and PPT application software

Submit your answer electronically via the Learning Management System.

- e.g. AB_BSBXCS402_Task 3 Cybersecurity awareness program_v1.0

Part C Arrange delivery of the cybersecurity awareness program

You are now required to arrange the training and information updates in the workplace of the cybersecurity awareness you developed in part B of this assessment task.

You will need to provide evidence of delivering this training to the workplace. This may include PowerPoint/slides, video evidence, phishing emails etc.

Your evidence will reflect the training program that you designed in Part B

Submit your evidence electronically via the Learning Management System.

- **e.g. AB_BSBXCS402_Task 3 Delivery of the cybersecurity program _v1.0**

Assessment Checklist: Task 3 - Supporting cyber security practices in the workplace

Learner name		**Learner ID**	
Assessor name		**Date**	

ASSESSMENT CHECKLIST

ASSESSOR TO COMPLETE THE FOLLOWING

DOCUMENTS

	The LEARNER submitted:	**SATISFACTORY**	**NOT SATISFACTORY**
	The completed Cybersecurity Awareness Survey from 6 people a range of different disciplines within the organisation (e.g. finance, administration, legal etc).	☐	☐
	The 6 recordings of the consultation with the 6 colleagues	☐	☐
	Correctly answered all sections of the Cybersecurity Finding Review Report	☐	☐
	Developed a Cybersecurity awareness Program relating to 2 different cyber security matters and answered all sections of the Cybersecurity awareness Program template	☐	☐
	Evidence of having successfully implemented the Cybersecurity awareness Program	☐	☐

Feedback:

Assessment Task Summary: Task 3 - Supporting cyber security practices in the workplace

TRAINER/ASSESSOR TO COMPLETE THE FOLLOWING: **THE LEARNER:**		YES	NO
1.	Satisfactorily completed all items in Assessment Checklist	☐	☐
FEEDBACK - Assessor must include feedback			
OVERALL TASK RESULT			
☐ Satisfactory ☐ Not Satisfactory (resubmission required) – Due date: _____			
DATE ASSESSMENT RETURNED			
TRAINER/ASSESSOR NAME			
TRAINER/ASSESSOR SIGNATURE	X		
LEARNER DECLARATION: PLEASE READ AND SIGN BELOW			
I, _____ have been advised of the outcome of this assessment task. PRINT NAME			
LEARNER SIGNATURE	X	DATE	

2

Consult with stakeholders

3. You are now required to interview a **minimum of 2 people in the work area. Record your interview with each of the 2 people. This may be done as a group consultation however each person will need to complete the survey form.**

   It is important to obtain information from people working in a range of different disciplines within the organisation (e.g.; finance, administration, legal etc).

4. You will now collate and review the information you have obtained and provide a report for management about the findings. Your report will need to use clear, specific and industry-related terminology relating to cyber security

Upload your solution to the BSBXCS Moodle shell Assessment Task 3

File Naming Convention:

BSBXCS402 AT3 ***Student Name & Student Number***.docx

Cyber Security Finding Review Report		
Overview of findings from information gathered from work area - including current trends identified in the work areas cybersecurity awareness and workplace practice of the staff.		
In the assessment of the workplace, we have discovered several aspects that are related to cyber security awareness and workplace procedures. This information is crucial that all employees understand of the current cyber security threats and how they can impact the company and their clients and how to avoid being a victim. 1. Phishing scams: Some employees have raised concerns regarding phishing emails and how to spot them I would strongly recommend training to prevent any malware or attacks. 2. Social engineering: During the investigation I discovered several staff members had either little or no knowledge of baiting and other social engineering scams 3. Password Requirements: I discovered there are no requirements for password complexity or minimum requirements for password some employees even allow other employees they no to know their username and password to login to complete tasks.		
Examples where current practice is complying with organisational policies and procedures: 1. During the investigation we discovered the organisation is complying with regular training to educate employees regarding the policy and procedures in the workplace 2. Regular software updates and patches are applied to keep the system UpToDate and protected		
2 Cybersecurity work practices or awareness that do not align with the organisation's policies and procedures or best practice (Potential threats)		Potential impact on the company
4.	Not implanting a training program regarding updated policies and procedures in the code of ethics as it is being updated in the organisation and where to find this information.	This can result in procedure not being implemented correctly such as not following password polies and procedures can result in unauthorised access to the organisations client's sensitive data and can damage the company's reputation

5.	Not educating employees of the potential threats and how to respond	Potential data leak or attack with a malicious code
Suggested ways to improve cybersecurity awareness for each of the 2 potential threats identified		
4.	Regularly implement training exercises and training plains to assess and improve the employees knowledge of what polices apply to them and why it is important to follow the code of ethics and where to find this information.	
5.	Educate employees and run training exercises on how to identify potential threats to the company and how to respond or report the incident.	

Submit your answers electronically via the Learning Management System.

- **e.g. AB_BSBXCS402_Task 3 Cyber Security Finding Review Report _v1.0**

Part B Create Cybersecurity awareness program about 2 cyber security matters.

Based on your report you are required to develop a cybersecurity awareness program for colleagues that support and promote cybersecurity practice and awareness in relation to **2 different cyber security matters.**

CYBERSECURITY AWARENESS PROGRAM	
Trainer Name:	
Planned training date:	
Planned training time from/to:	7.30am – 12.30pm
Cyber Security Matter 1: *Phishing email scam awareness training.*	
Cyber Security Matter 2: Insider threat and awareness training.	
Objectives of the training to meet organisation-wide practice: • Raise awareness regarding cyber security awareness. • Educate working on how to spot phishing scams.	
Skills to be developed: • Recognizing phishing scam emails. • how to respond to appropriately to phishing attacks • how to report potential threats	**Knowledge to be developed:** • What kinds of phishing scams and their methods • How to follow the organisations policies and procedures related to phishing incidents
Training method/s: • Interactive presentations • Handouts/exercises • Real life case studies • Group discussions or individual discussions	
Simulated training method (list the technology platforms to assist with promoting cyber security) :	

• Phishing scam simulation platform • Insider threat simulation • Learning management system with cyber security training modules		
Training location: Avengers office		
Training activities		**Resources required**
1.	Case studies	Detailed case study scenarios Background information Supporting documentation
2.	Exercises and simulations	Presentation slides Handouts / worksheets
3.	Group and individual discussions with work and Q&A	Trained instructors/experts facilities

Submit your answer electronically via the Learning Management System.

- e.g. AB_BSBXCS402_Task 3 Cybersecurity awareness program_v1.0

Part C Arrange delivery of the cybersecurity awareness program

You are now required to arrange the training and information updates in the workplace of the cybersecurity awareness you developed in part B of this assessment task.

You will need to provide evidence of delivering this training to the workplace. This may include PowerPoint/slides, video evidence, phishing emails etc.

Your evidence will reflect the training program that you designed in Part B

Submit your evidence electronically via the Learning Management System.

- **e.g. AB_BSBXCS402_Task 3 Delivery of the cybersecurity program _v1.0**

Assessment Checklist: Task 3 - Supporting cyber security practices in the workplace

Learner name		**Learner ID**	
Assessor name		**Date**	

ASSESSMENT CHECKLIST

ASSESSOR TO COMPLETE THE FOLLOWING

DOCUMENTS

	The LEARNER submitted:	**SATISFACTORY**	**NOT SATISFACTORY**
	The completed Cybersecurity Awareness Survey from 2 people a range of different disciplines within the organisation (e.g. finance, administration, legal etc).	☐	☐
	The 2 recordings of the consultation with the 2 colleagues	☐	☐
	Correctly answered all sections of the Cybersecurity Finding Review Report	☐	☐
	Developed a Cybersecurity awareness Program relating to 2 different cyber security matters and answered all sections of the Cybersecurity awareness Program template	☐	☐
	Evidence of having successfully implemented the Cybersecurity awareness Program	☐	☐

Feedback:

Assessment Task Summary: Task 3 - Supporting cyber security practices in the workplace

TRAINER/ASSESSOR TO COMPLETE THE FOLLOWING: **THE LEARNER:**		YES	NO
1.	Satisfactorily completed all items in Assessment Checklist	☐	☐
FEEDBACK - Assessor must include feedback			
OVERALL TASK RESULT			
☐ Satisfactory ☐ Not Satisfactory (resubmission required) – Due date: _____			
DATE ASSESSMENT RETURNED			
TRAINER/ASSESSOR NAME			
TRAINER/ASSESSOR SIGNATURE	X		
LEARNER DECLARATION: PLEASE READ AND SIGN BELOW			
I, _____ have been advised of the outcome of this assessment task. PRINT NAME			
LEARNER SIGNATURE	X	DATE	

3

Consult with stakeholders

5. You are now required to interview a **minimum of 6 people in the work area. Record your interview with each of the 6 people. This may be done as a group consultation however each person will need to complete the survey form.**

   It is important to obtain information from people working in a range of different disciplines within the organisation (e.g.; finance, administration, legal etc).

6. You will now collate and review the information you have obtained and provide a report for management about the findings. Your report will need to use clear, specific and industry-related terminology relating to cyber security

Upload your solution to the BSBXCS Moodle shell Assessment Task 3

File Naming Convention:

BSBXCS402 AT3 ***Student Name & Student Number***.docx

Cyber Security Finding Review Report		
Overview of findings from information gathered from work area - including current trends identified in the work areas cybersecurity awareness and workplace practice of the staff.		
It's already known that cyber Security is a process that's designed to protect networks and devices from external threats. Businesses typically employ Cyber Security professionals to protect their confidential information, maintain employee productivity, and enhance customer confidence in products and services. The following is the overview of findings from information gathered including current trends identified in the work areas cybersecurity awareness and workplace practice of the staff • Denial of Service, or DOS Where a hacker consumes all of a server's resources, so there's nothing for legitimate users to access • Malware Where victims are hit with a worm or virus that renders their devices useless • Man in the Middle Attack Where a hacker puts himself between a victim's machine and a router to sniff data packets• Phishing Where a hacker sends a seemingly legitimate-looking email asking users to disclose personal information		
Examples where current practice is complying with organisational policies and procedures: • Keeping company's software up to date • Using anti-virus protection & firewall • Using strong passwords & use a password management tool • Using two-factor or multi-factor authentication. • Learning about phishing scams – be very suspicious of emails, phone calls, and flyers.		
3 Cybersecurity work practices or awareness that do not align with the organisation's policies and procedures or best practice (Potential threats)		Potential impact on the company
6.	Organizing employees' training on cyber security	When employees don't have the best security awareness training, they can't be more likely to promptly trace potential threats and report any incoming incidents.
7.	Use multifactor identification	Without multi-factor authentication (MFA), cybercriminals can much more

		easily gain access to employee's accounts.
8.	Enforcing safe password practices	The stronger your password, the more protected your computer will be from hackers and malicious software. Employees should maintain strong passwords for all accounts on their computers.
Suggested ways to improve cybersecurity awareness for each of the 3 potential threats identified		
6.	Using anti-virus protection & firewall	
7.	Using anti-virus protection & firewall	
8.	Learning about phishing scams – be very suspicious of emails, phone calls, and flyers.	

Submit your answers electronically via the Learning Management System.

- **e.g. AB_BSBXCS402_Task 3 Cyber Security Finding Review Report _v1.0**

Part B Create Cybersecurity awareness program about 2 cyber security matters.

Based on your report you are required to develop a cybersecurity awareness program for colleagues that support and promote cybersecurity practice and awareness in relation to **2 different cyber security matters.**

CYBERSECURITY AWARENESS PROGRAM	
Trainer Name:	
Planned training date:	
Planned training time from/to:	10am – 11:30am
Cyber Security Matter 1: Denial of Service (DOS) attack	
Cyber Security Matter 2 Phishing attack**:**	
Objectives of the training to meet organisation-wide practice:	

The main objective of the training is to formally educating a workforce on the various cyber threats that exist, how to recognize them, and steps to take to keep themselves and their company safe. • Train on how to use an anti-virus program • Identification of phishing emails	
Skills to be developed: Keep up with cybersecurity compliance regulations • Prevent employees from falling for phishing scams	**Knowledge to be developed:** Incorporate cybersecurity into the company culture • Reduce the likelihood of a successful breach
Training method/s: Demonstration • Explanation • Showing videos • Providing examples • Research and discussion	
Simulated training method (list the technology platforms to assist with promoting cyber security) :The following security platforms will offer well-defined and flexible options for responding to and mitigating threats, including automated and manual options. Examples of penetration testing tools and platforms include Anti-malware software, Metasploit, Kali Linux, Zoom meetings, Windows defender firewall etc…	
Training location: Trainings Hall	

Training activities		**Resources required**
1.	Present the PTT and show the Video	Computer and PPT application software
2.	Discuss the video and presentationn	Video software, workplace policies and procedures
3.	Show how to run the anti-virus program	Anti-virus program
4.	Ask participants to run the program themselves	Workplace policies and procedures, Antivirus program
5.	Test their knowledgee	Workplace policies and procedures, Antivirus program

6.		

Submit your answer electronically via the Learning Management System.

- e.g. AB_BSBXCS402_Task 3 Cybersecurity awareness program_v1.0

Part C Arrange delivery of the cybersecurity awareness program

You are now required to arrange the training and information updates in the workplace of the cybersecurity awareness you developed in part B of this assessment task.

You will need to provide evidence of delivering this training to the workplace. This may include PowerPoint/slides, video evidence, phishing emails etc.

Your evidence will reflect the training program that you designed in Part B

Submit your evidence electronically via the Learning Management System.

- **e.g. AB_BSBXCS402_Task 3 Delivery of the cybersecurity program _v1.0**

Assessment Checklist: Task 3 - Supporting cyber security practices in the workplace

Learner name		**Learner ID**	
Assessor name		**Date**	

ASSESSMENT CHECKLIST

ASSESSOR TO COMPLETE THE FOLLOWING

DOCUMENTS

	The LEARNER submitted:	**SATISFACTORY**	**NOT SATISFACTORY**
	The completed Cybersecurity Awareness Survey from 6 people a range of different disciplines within the organisation (e.g. finance, administration, legal etc).	☐	☐
	The 6 recordings of the consultation with the 6 colleagues	☐	☐
	Correctly answered all sections of the Cybersecurity Finding Review Report	☐	☐
	Developed a Cybersecurity awareness Program relating to 2 different cyber security matters and answered all sections of the Cybersecurity awareness Program template	☐	☐
	Evidence of having successfully implemented the Cybersecurity awareness Program	☐	☐

Feedback:

Assessment Task Summary: Task 3 - Supporting cyber security practices in the workplace

TRAINER/ASSESSOR TO COMPLETE THE FOLLOWING: **THE LEARNER:**		YES	NO
1.	Satisfactorily completed all items in Assessment Checklist	☐	☐
FEEDBACK - Assessor must include feedback			
OVERALL TASK RESULT			
☐ Satisfactory ☐ Not Satisfactory (resubmission required) – Due date: _____			
DATE ASSESSMENT RETURNED			
TRAINER/ASSESSOR NAME			
TRAINER/ASSESSOR SIGNATURE	X		
LEARNER DECLARATION: PLEASE READ AND SIGN BELOW			
I, _____ have been advised of the outcome of this assessment task. PRINT NAME			
LEARNER SIGNATURE	X	DATE	

4

Consult with stakeholders

7. You are now required to interview a **minimum of 2 people in the work area. Record your interview with each of the 2 people. This may be done as a group consultation however each person will need to complete the survey form.**

   It is important to obtain information from people working in a range of different disciplines within the organisation (e.g.; finance, administration, legal etc).

8. You will now collate and review the information you have obtained and provide a report for management about the findings. Your report will need to use clear, specific and industry-related terminology relating to cyber security

Upload your solution to the BSBXCS Moodle shell Assessment Task 3

File Naming Convention:

BSBXCS402 AT3 ***Student Name & Student Number***.docx

Cyber Security Finding Review Report
Overview of findings from information gathered from work area - including current trends identified in the work areas cybersecurity awareness and workplace practice of the staff.
Overview of Findings: We conducted an assessment to understand how well our staff is aware of cybersecurity and how effectively they practice it in the workplace. Here are the key takeaways: **1. Cybersecurity Awareness:** Secure Information Handling: Our staff is generally good at securely storing and sharing information. However, there's room to reinforce this practice. Encryption and Protocols: Most employees are familiar with encryption and secure communication methods, especially for sensitive data. Data Classification and Management: Our employees understand the importance of classifying data by sensitivity and managing it accordingly, especially when it comes to financial data. Data Governance: Our team is well aware of our data governance policies, including access controls, data retention, and secure data disposal. **2. Workplace Practices:** Current Trends: We're keeping up with the latest trends in cybersecurity, particularly in response to increased remote work and cloud services usage. Training and Awareness: Our staff has access to cybersecurity training, and there's a culture of continuous learning and awareness-building.

Incident Response: We have robust procedures in place to respond to cybersecurity incidents, ensuring minimal impact.

Regulatory Compliance: We're fully compliant with industry-specific regulations, like [mention specific regulations].

Recommendations:

To further strengthen our cybersecurity:

Continue training and awareness programs.

Enhance remote work security.

Assess third-party vendors and cloud service providers.

Regularly test incident response procedures.

Conclusion:

Our organization is committed to cybersecurity awareness and best practices. By making minor enhancements and staying proactive, we can strengthen our cybersecurity even further.

This overview simplifies the key findings and recommendations, making them easy to grasp for all stakeholders.

Examples where current practice is complying with organisational policies and procedures:

Keeping Important Information Safe: The company says we should keep important information safe. People in the company are doing just that - they make sure that important data is protected and not shared with anyone who shouldn't see it.

Strong Passwords: The company's rule is to use strong passwords that are hard for others to guess. Everyone is following this rule by creating strong passwords and changing them regularly. They don't write down their passwords or share them with others.

2 Cybersecurity work practices or awareness that do not align with the organisation's policies and procedures or best practice (Potential threats)		Potential impact on the company
9.	Some employees are using weak and easily guessable passwords for their accounts, which goes against the organization's password policy that mandates strong and complex passwords.	Weak passwords are vulnerable to brute-force attacks and unauthorized access. If attackers guess these passwords, they could gain access to sensitive information, compromising data security.
10.	A few employees occasionally use their personal devices, such as smartphones and laptops, to access work-related information without using the organization's secure remote access procedures.	Unsecured personal devices may lack up-to-date security measures, making them potential entry points for cyber threats. If malware or viruses infect these devices, it could lead to data breaches or network compromises.
Suggested ways to improve cybersecurity awareness for each of the 2 potential threats identified		
9.	Mandatory Password Policy Training: Conduct mandatory training sessions for all employees to educate them about the importance of strong passwords and how to create and manage them effectively. Ensure they understand the organization's password policy.	
10.	BYOD (Bring Your Own Device) Policy: Develop and enforce a BYOD policy that outlines specific security requirements for personal devices used for work. This policy should include guidelines for device security, such as enabling screen locks, encryption, and regular updates.	

Submit your answers electronically via the Learning Management System.

- **e.g. AB_BSBXCS402_Task 3 Cyber Security Finding Review Report _v1.0**

Part B Create Cybersecurity awareness program about 2 cyber security matters.

Based on your report you are required to develop a cybersecurity awareness program for colleagues that support and promote cybersecurity practice and awareness in relation to **2 different cyber security matters.**

CYBERSECURITY AWARENESS PROGRAM	
Trainer Name:	
Planned training date:	
Planned training time from/to:	13:00-14:00
Cyber Security Matter 1: **Password Security**	
Cyber Security Matter 2: **BYOD (Bring Your Own Device) Security**	
Objectives of the training to meet organisation-wide practice: To educate participants on the importance of strong and secure passwords. To ensure that all participants understand and can implement the organization's password policy. To raise awareness about the risks associated with weak passwords and password reuse. To empower participants to enable Multi-Factor Authentication (MFA) on their work accounts. To familiarize participants with BYOD policy and its significance. To provide guidance on securing personal devices used for work. To promote the use of security tools and apps for BYOD security. To emphasize the reporting and compliance requirements for BYOD incidents.	
Skills to be developed: Creating strong and unique passwords. Managing passwords effectively. Enabling and using Multi-Factor Authentication (MFA). Implementing security practices on personal devices. Recognizing and reporting BYOD-related incidents.	**Knowledge to be developed:** Understanding the importance of password security. Comprehending the organization's password policy. Recognizing the risks associated with weak passwords. Knowing how to secure personal devices for work. Familiarity with BYOD policy and reporting procedures.
Training method/s: In-person workshops Webinars	

Interactive discussions Hands-on exercises Q&A sessions Case studies
Simulated training method (list the technology platforms to assist with promoting cyber security) : Password management tools (e.g., LastPass, Dashlane) Multi-Factor Authentication (MFA) setup BYOD security apps and tools Simulated phishing exercises (for password security)
Training location: office

Training activities		**Resources required**
1.	Slides covering password security and BYOD security. Visual aids for demonstrations.	Presentation Materials
2.	Information and guidance on recommended security apps/tools.	BYOD Security Tools
3.	Relevant case studies illustrating the importance of password security and BYOD security.	Case Studies

Submit your answer electronically via the Learning Management System.

- e.g. AB_BSBXCS402_Task 3 Cybersecurity awareness program_v1.0

Part C Arrange delivery of the cybersecurity awareness program

You are now required to arrange the training and information updates in the workplace of the cybersecurity awareness you developed in part B of this assessment task.

You will need to provide evidence of delivering this training to the workplace. This may include PowerPoint/slides, video evidence, phishing emails etc.

Your evidence will reflect the training program that you designed in Part B

PowerPoint is prepared sepalately in same file.

Submit your evidence electronically via the Learning Management System.

- **e.g. AB_BSBXCS402_Task 3 Delivery of the cybersecurity program _v1.0**

Assessment Checklist: Task 3 - Supporting cyber security practices in the workplace

Learner name		**Learner ID**	
Assessor name		**Date**	

ASSESSMENT CHECKLIST

ASSESSOR TO COMPLETE THE FOLLOWING

DOCUMENTS

	The LEARNER submitted:	**SATISFACTORY**	**NOT SATISFACTORY**
	The completed Cybersecurity Awareness Survey from 2 people a range of different disciplines within the organisation (e.g. finance, administration, legal etc).	☐	☐
	The 2 recordings of the consultation with the 2 colleagues	☐	☐
	Correctly answered all sections of the Cybersecurity Finding Review Report	☐	☐
	Developed a Cybersecurity awareness Program relating to 2 different cyber security matters and answered all sections of the Cybersecurity awareness Program template	☐	☐
	Evidence of having successfully implemented the Cybersecurity awareness Program	☐	☐

Feedback:

Assessment Task Summary: Task 3 - Supporting cyber security practices in the workplace

TRAINER/ASSESSOR TO COMPLETE THE FOLLOWING: **THE LEARNER:**		YES	NO
1.	Satisfactorily completed all items in Assessment Checklist	☐	☐
FEEDBACK - Assessor must include feedback			
OVERALL TASK RESULT			
☐ Satisfactory ☐ Not Satisfactory (resubmission required) – Due date: _____			
DATE ASSESSMENT RETURNED			
TRAINER/ASSESSOR NAME			
TRAINER/ASSESSOR SIGNATURE	X		
LEARNER DECLARATION: PLEASE READ AND SIGN BELOW			
I, _____ have been advised of the outcome of this assessment task. PRINT NAME			
LEARNER SIGNATURE	X	DATE	