DEERFIELD
BEACH
POLICE

POLICE DEPARTMENT

Aadith Preetham

“Week 2 Deliverables”

“Due Date”

23rd January 2025

Introduction

The **Deerfield Beach Police Department (DBPD)** is committed to ensuring that our employees are well-versed in the importance of **cyber security** as it pertains to their daily work. This project aims to create an engaging and informative **online quiz** that will help us assess the knowledge of our staff regarding cyber security policies, procedures, and protocols.

The **Cyber Security Knowledge Survey** is designed to identify any gaps in employees' understanding of critical cyber security practices and ensure that they are equipped with the knowledge necessary to protect department assets and sensitive information. This will be achieved by testing employees on a variety of topics, such as password management, phishing prevention, data protection, and incident response.

The survey will employ **gamification techniques** to foster a fun and engaging environment for learning, motivating employees to participate and perform their best. By completing this survey, DBPD staff will not only improve their cyber security awareness but also contribute to a safer, more secure working environment for the entire department.

Objectives and Scope of the Survey

- **Target Audience** All **Deerfield Beach Police Department employees**, including officers, administrative staff, and IT personnel, will participate in the survey.
- **Core Topics Covered**: The survey will assess knowledge across key areas of cyber security, including:
  - Cyber security policies and procedures
  - Data protection and privacy laws
  - Incident response protocols
  - Best practices for network security

- Compliance with state and federal regulations

- **Expected Outcomes**
  - Identify areas where additional training is needed
  - Encourage a department-wide culture of security awareness
  - Improve adherence to established policies and protocols

- **Implementation and Roll-Out Plan**
- **Timeline**

  The survey will be developed, tested, and launched over the course of one week.
  - **Day 1-2:** Design and development of the survey questions and gamification elements.
  - **Day 3-4:** Testing the survey platform and ensuring compatibility across devices.
  - **Day 5:** Launch of the survey to all department employees, with reminders to ensure full participation.
  - **Day 6-7:** Analysis of responses and preparation of feedback for participants.
- **Communication Plan**
  - Clear instructions will be sent to employees outlining how to participate in the survey, along with a reminder of the importance of cyber security in their daily operations.
  - **Incentives:** Employees will be motivated through incentives, such as **recognition in department communications**, and prizes for high scorers to encourage participation.

Survey Questionnaire (Full Version)

DEERFIELD BEACH POLICE DEPARTMENT: CYBER SECURITY KNOWLEDGE SURVEY

Welcome to the **Deerfield Beach Police Department Cyber Security Knowledge Survey**! This quiz is designed to assess your understanding of the department's cyber security protocols, policies, and best practices. As cyber threats evolve, it is crucial that all staff members stay up-to-date with the latest guidelines to ensure the safety and integrity of our systems.

This interactive quiz will test your knowledge on topics ranging from password management and phishing awareness to data protection and incident response. As you progress through the questions, you'll encounter engaging challenges and scenarios to help reinforce your learning.

Upon completion, you'll receive personalized feedback and tips to further enhance your cyber security awareness. Let's ensure that we are all equipped to protect the sensitive information and resources that we work with every day.

Your participation in this survey is vital to strengthen our collective defense against cyber threats. Let's stay secure, informed, and vigilant!

* Indicates required question

1. Email *

____

2. **Q1:** What is the minimum recommended length for a strong password? * 0 points

Tick all that apply.

□ A) 6 characters

□ B) 8 characters

□ C) 12 characters

□ D) 16 characters

3. **Q2:** Which of the following is considered a best practice for password management?

Mark only one oval.

○ A) Using the same password for multiple accounts

○ B)Writing passwords down on paper

○ C) Enabling multi-factor authentication (MFA)

○ D) Sharing your password with a colleague if you're on leave

4. **Q3:** Which of the following password policies is most secure? * 0 points

Mark only one oval.

○ A) Using a simple word like "password123"

○ B)Using a combination of uppercase, lowercase, numbers, and symbols

○ C) Reusing passwords across different accounts

○ D) Changing passwords once every year

5. **Q4:** What is phishing? * 0 points

Mark only one oval.

○ A) A technique to secure sensitive data

○ B)A method of tricking individuals into disclosing confidential information

○ C) A form of hacking into secure networks

○ D) A process of protecting emails from cyber threats

6. **Q5:** Which of the following is a red flag of a phishing email? *

Mark only one oval.

○ A) The email comes from a known source

○ B)The email asks you to click on a link to verify your account

○ C) The email has a subject line related to a task you already completed

○ D) The email uses proper grammar and spelling

7. **Q6:** If you receive an email with an urgent request for sensitive information, what should you do? * 0 points

Mark only one oval.

○ A) Reply immediately with the requested information

○ B)Open any attachments to verify the sender

○ C) Forward the email to your supervisor and delete it

○ D) Ignore it and continue working as usual

8. **Q7:** What does "data encryption" refer to? * 0 points

Mark only one oval.

○ A) The process of deleting sensitive information

○ B)The process of converting data into a code to prevent unauthorized access

○ C) The process of storing data in cloud systems

○ D) The process of backing up data regularly

9. **Q8:** What is the best way to protect personal and department data when accessing it from a public Wi-Fi network?

Mark only one oval.

○ A) Use a virtual private network (VPN)

○ B)Only access public social media

○ C) Log in without a password

○ D) Turn off your device's security features

10. **Q9:** Which of the following actions could lead to a data breach? * 0 points

Mark only one oval.

○ A) Encrypting sensitive files

○ B) Sharing your login credentials over the phone

○ C) Using a password manager

○ D) Backing up important data to a secure cloud server

11. **Q10:** What should you do if you notice unusual activity on a department computer? * 0 points

Mark only one oval.

○ A) Ignore it and continue working

○ B) Disconnect the device from the network and report it immediately

○ C) Try to fix the issue yourself

○ D) Email the suspicious activity to your colleagues for feedback

12. **Q11:** In the event of a cyber security incident, what is the first action you should take?

Mark only one oval.

○ A) Inform the media

○ B) Document the incident and inform your supervisor or IT department

○ C) Restart the device to remove traces

○ D) Try to resolve the issue on your own

13. **Q12:** If you suspect your account has been compromised, what should you * 0 points do immediately?

Mark only one oval.

○ A) Change your password and notify IT support

○ B) Ignore it unless you notice something serious

○ C) Log out and wait to see if it resolves itself

○ D) Delete all your emails and files

14. **Q13:** Which of the following is a key objective of the Deerfield Beach Police * 0 points Department's cyber security policies?

Mark only one oval.

○ A) To ensure secure and timely data access for officers

○ B) To promote the use of personal devices on the network

○ C) To protect confidential information and prevent unauthorized access

○ D) To allow unrestricted internet browsing for all employees

15. **Q14:** According to department policy, what is required when using personal devices to access work-related data?

Mark only one oval.

○ A) No special requirements

○ B) Ensure your device is equipped with anti-virus software

○ C) Use public Wi-Fi for easy access

○ D) Share the device login credentials with your colleagues

16. **Q15:** What should you do with sensitive information you no longer need to * 0 points access?

Mark only one oval.

○ A) Delete it without any further action

○ B) Shred physical copies and securely delete digital files

○ C) Store it on your local hard drive

○ D) Leave it in your inbox for future reference

17. **Q16:** Why is regular cyber security training essential for police department * 0 points staff?

Mark only one oval.

○ A) To avoid using outdated software

○ B) To comply with state and federal regulations

○ C) To ensure all employees know how to use the internet

○ D) To increase the risk of potential cyber threats

18. **Q17:** What should be included in a secure email protocol at the Deerfield Beach Police Department?

Mark only one oval.

○ A) Sending sensitive documents as unencrypted attachments

○ B) Using a secure email service and encryption when sending
○ sensitive information

○ C) Sharing all departmental passwords via email

D) Using your personal email to send work-related documents

19. **Q18:** What is the purpose of conducting regular security audits within the * 0 points police department?

Mark only one oval.

○ A) To identify and mitigate potential security vulnerabilities

○ B) To check the internet usage of employees

○ C) To monitor email traffic

○ D) To assess the physical security of office spaces

20. **Q19:** Which Florida cyber security law requires government agencies, * 0 points including police departments, to establish and maintain security controls to protect public records?

Mark only one oval.

○ A) Florida Information Protection Act (FIPA)

○ B) Florida Government Cybersecurity Act

○ C) Florida Public Records Law

○ D) Florida Digital Privacy Act

21. **Q20:** Which of the following actions can help the department maintain compliance with cyber security laws and regulations?

Mark only one oval.

○ A) Ignoring software updates to save time

○ B) Regularly updating software and conducting vulnerability assessments

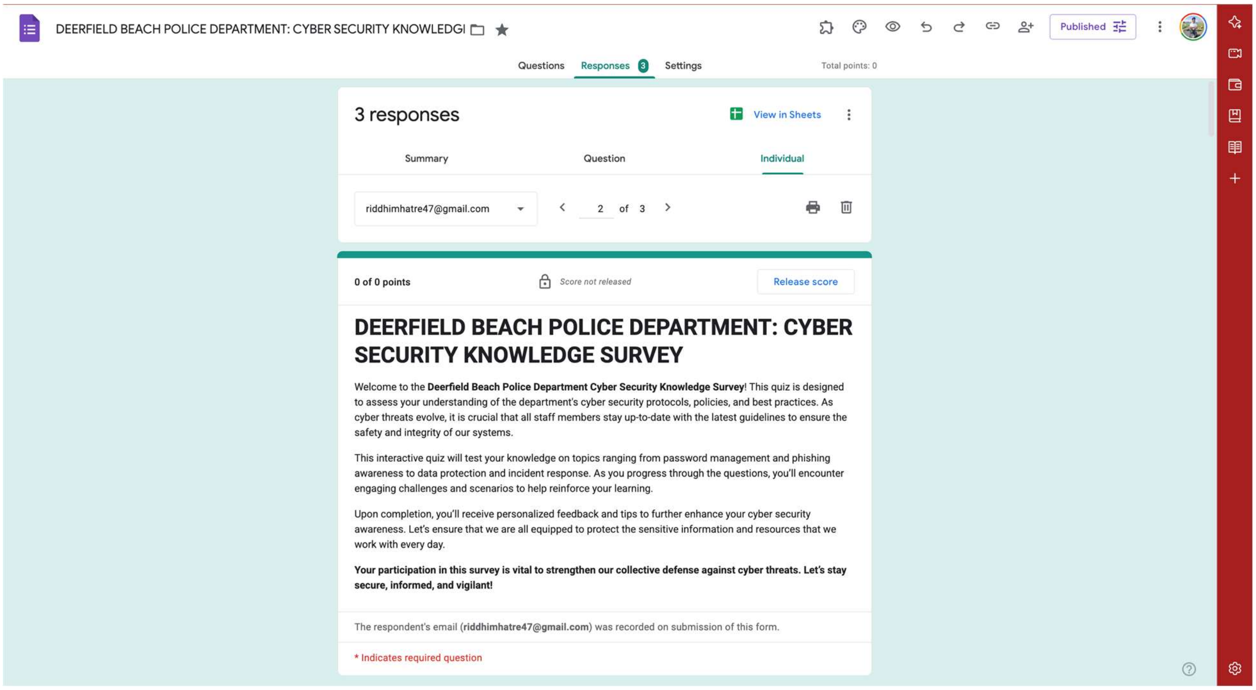
○ C) Using outdated encryption protocols for faster communication

○ D) Reducing the frequency of security audits

This content is neither created nor endorsed by Google.

Google Forms

Survey Results (Sample Data)



DEERFIELD BEACH POLICE DEPARTMENT: CYBER SECURITY KNOWLEDGI

Total points: 0

3 responses

riddhimhatre47@gmail.com

2 of 3

0 of 0 points

Score not released

DEERFIELD BEACH POLICE DEPARTMENT: CYBER SECURITY KNOWLEDGE SURVEY

Welcome to the **Deerfield Beach Police Department Cyber Security Knowledge Survey**! This quiz is designed to assess your understanding of the department's cyber security protocols, policies, and best practices. As cyber threats evolve, it is crucial that all staff members stay up-to-date with the latest guidelines to ensure the safety and integrity of our systems.

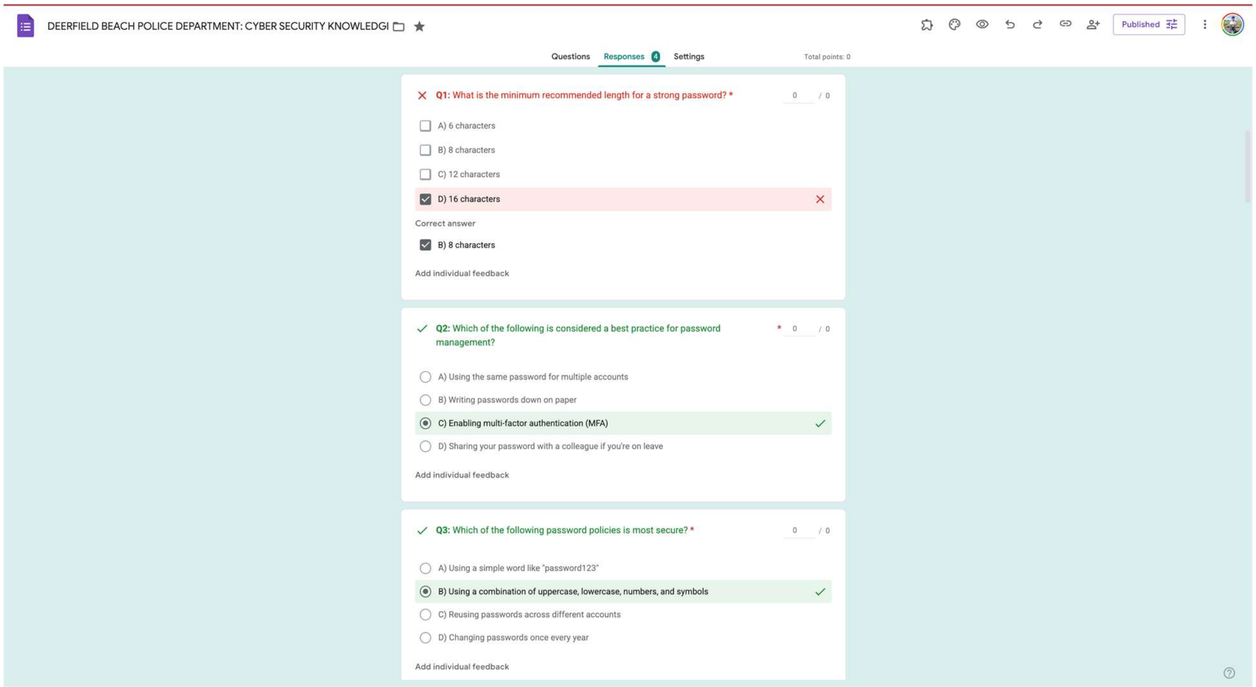
This interactive quiz will test your knowledge on topics ranging from password management and phishing awareness to data protection and incident response. As you progress through the questions, you'll encounter engaging challenges and scenarios to help reinforce your learning.

Upon completion, you'll receive personalized feedback and tips to further enhance your cyber security awareness. Let's ensure that we are all equipped to protect the sensitive information and resources that we work with every day.

Your participation in this survey is vital to strengthen our collective defense against cyber threats. Let's stay secure, informed, and vigilant!

The respondent's email (**riddhimhatre47@gmail.com**) was recorded on submission of this form.

* Indicates required question



DEERFIELD BEACH POLICE DEPARTMENT: CYBER SECURITY KNOWLEDGI

Total points: 0

☒ Q1: What is the minimum recommended length for a strong password? * 0 / 0

□ A) 6 characters

□ B) 8 characters

□ C) 12 characters

☑ D) 16 characters ✗

Correct answer

☑ B) 8 characters

Add individual feedback

✓ Q2: Which of the following is considered a best practice for password management? * 0 / 0

○ A) Using the same password for multiple accounts

○ B) Writing passwords down on paper

● C) Enabling multi-factor authentication (MFA) ✓

○ D) Sharing your password with a colleague if you're on leave

Add individual feedback

✓ Q3: Which of the following password policies is most secure? * 0 / 0

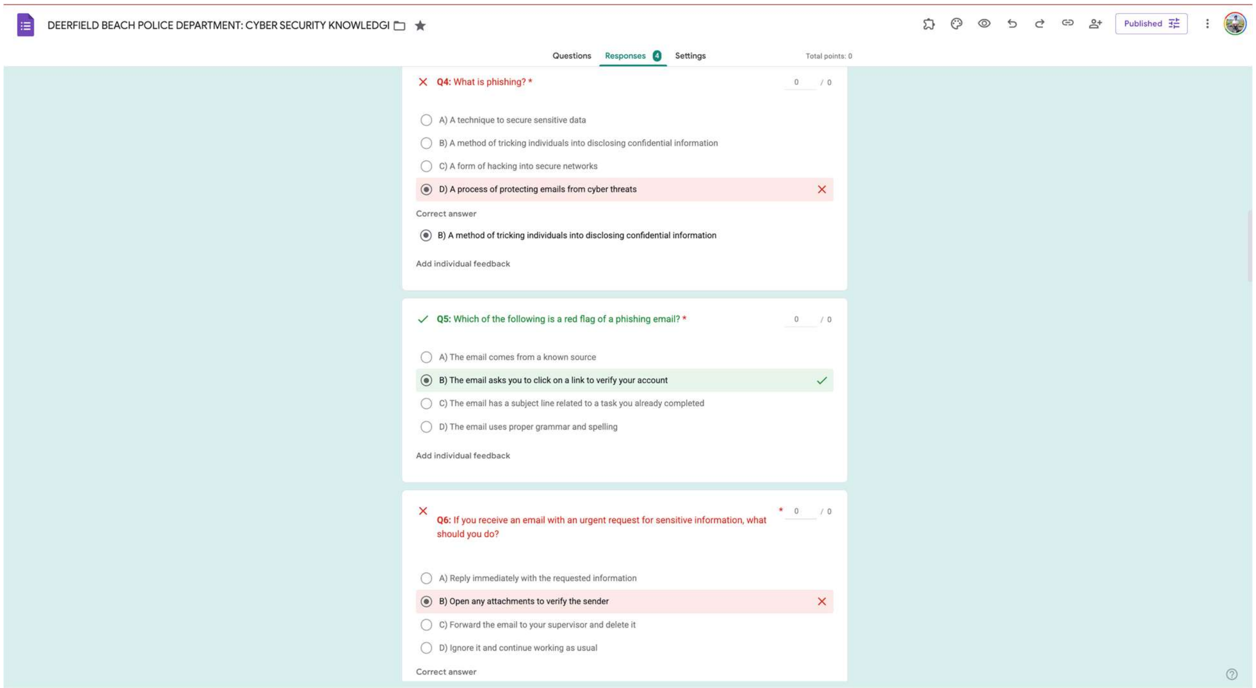
○ A) Using a simple word like "password123"

● B) Using a combination of uppercase, lowercase, numbers, and symbols ✓

○ C) Reusing passwords across different accounts

○ D) Changing passwords once every year

Add individual feedback



✗ **Q4:** What is phishing? * 0 / 0

○ A) A technique to secure sensitive data

○ B) A method of tricking individuals into disclosing confidential information

○ C) A form of hacking into secure networks

● D) A process of protecting emails from cyber threats ✗

Correct answer

● B) A method of tricking individuals into disclosing confidential information

Add individual feedback

✓ **Q5:** Which of the following is a red flag of a phishing email? * 0 / 0

○ A) The email comes from a known source

● B) The email asks you to click on a link to verify your account ✓

○ C) The email has a subject line related to a task you already completed

○ D) The email uses proper grammar and spelling

Add individual feedback

✗ **Q6:** If you receive an email with an urgent request for sensitive information, what should you do? * 0 / 0

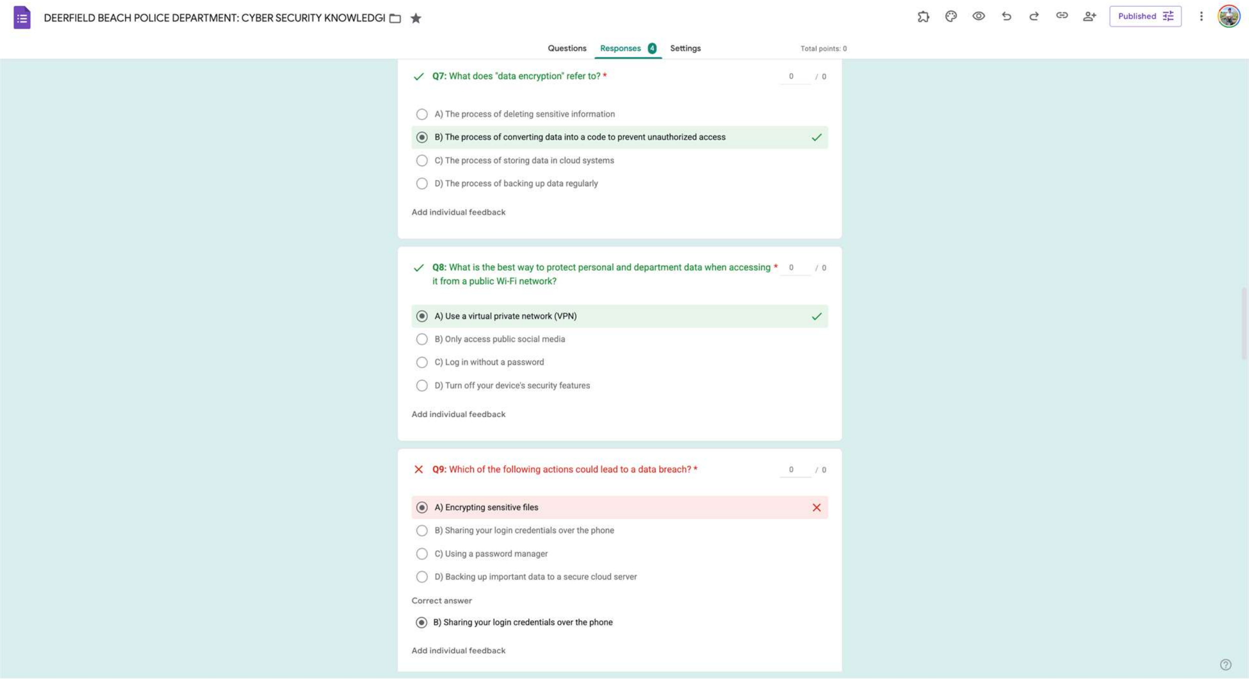
○ A) Reply immediately with the requested information

● B) Open any attachments to verify the sender ✗

○ C) Forward the email to your supervisor and delete it

○ D) Ignore it and continue working as usual

Correct answer



✓ **Q7:** What does "data encryption" refer to? * 0 / 0

○ A) The process of deleting sensitive information

● B) The process of converting data into a code to prevent unauthorized access ✓

○ C) The process of storing data in cloud systems

○ D) The process of backing up data regularly

Add individual feedback

✓ **Q8:** What is the best way to protect personal and department data when accessing it from a public Wi-Fi network? * 0 / 0

● A) Use a virtual private network (VPN) ✓

○ B) Only access public social media

○ C) Log in without a password

○ D) Turn off your device's security features

Add individual feedback

✗ **Q9:** Which of the following actions could lead to a data breach? * 0 / 0

● A) Encrypting sensitive files ✗

○ B) Sharing your login credentials over the phone

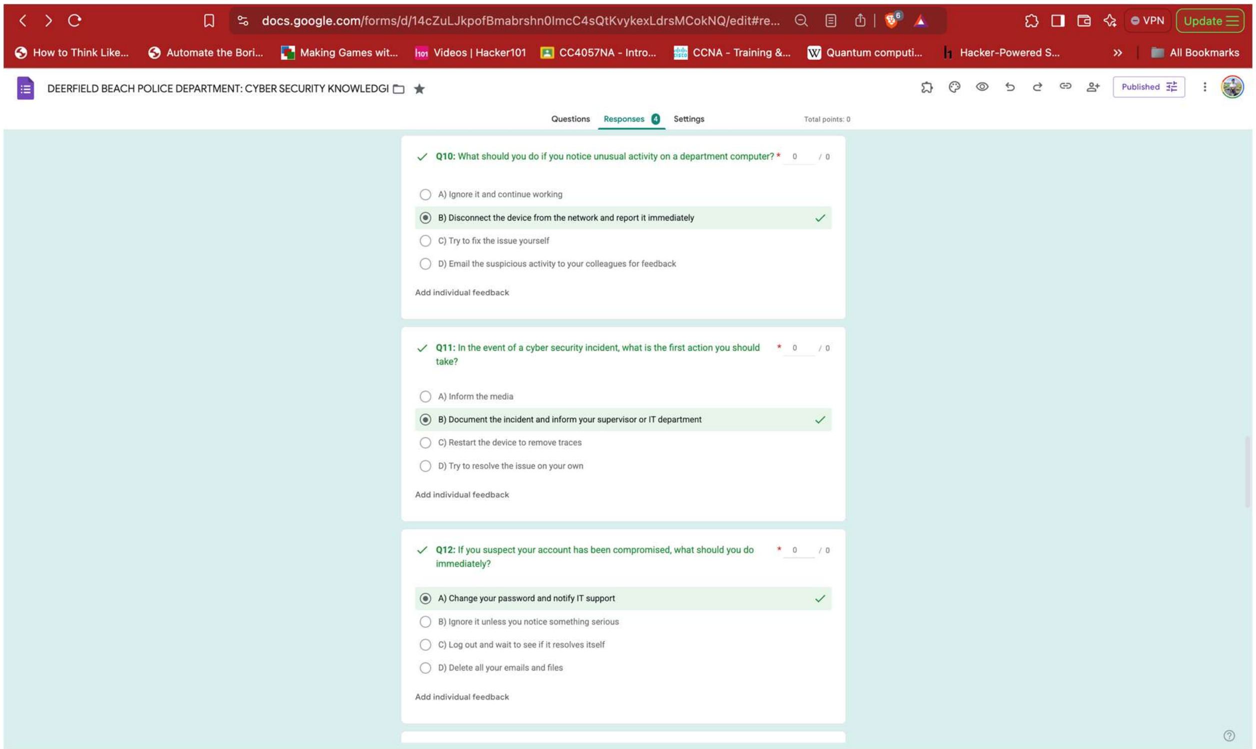
○ C) Using a password manager

○ D) Backing up important data to a secure cloud server

Correct answer

● B) Sharing your login credentials over the phone

Add individual feedback



DEERFIELD BEACH POLICE DEPARTMENT: CYBER SECURITY KNOWLEDGI

✓ **Q10:** What should you do if you notice unusual activity on a department computer? * 0 / 0

○ A) Ignore it and continue working

● B) Disconnect the device from the network and report it immediately ✓

○ C) Try to fix the issue yourself

○ D) Email the suspicious activity to your colleagues for feedback

Add individual feedback

✓ **Q11:** In the event of a cyber security incident, what is the first action you should take? * 0 / 0

○ A) Inform the media

● B) Document the incident and inform your supervisor or IT department ✓

○ C) Restart the device to remove traces

○ D) Try to resolve the issue on your own

Add individual feedback

✓ **Q12:** If you suspect your account has been compromised, what should you do immediately? * 0 / 0

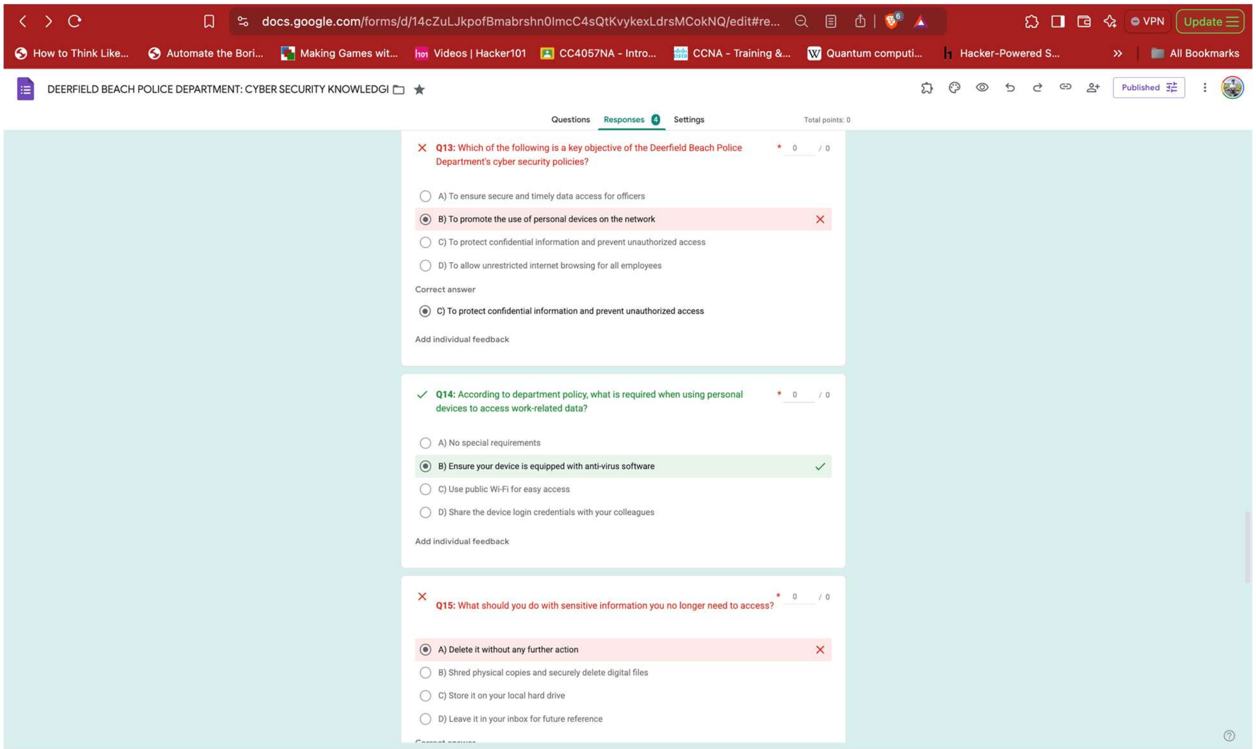
● A) Change your password and notify IT support ✓

○ B) Ignore it unless you notice something serious

○ C) Log out and wait to see if it resolves itself

○ D) Delete all your emails and files

Add individual feedback



DEERFIELD BEACH POLICE DEPARTMENT: CYBER SECURITY KNOWLEDGI

✗ **Q13:** Which of the following is a key objective of the Deerfield Beach Police Department's cyber security policies? * 0 / 0

○ A) To ensure secure and timely data access for officers

● B) To promote the use of personal devices on the network ✗

○ C) To protect confidential information and prevent unauthorized access

○ D) To allow unrestricted internet browsing for all employees

Correct answer

● C) To protect confidential information and prevent unauthorized access

Add individual feedback

✓ **Q14:** According to department policy, what is required when using personal devices to access work-related data? * 0 / 0

○ A) No special requirements

● B) Ensure your device is equipped with anti-virus software ✓

○ C) Use public Wi-Fi for easy access

○ D) Share the device login credentials with your colleagues

Add individual feedback

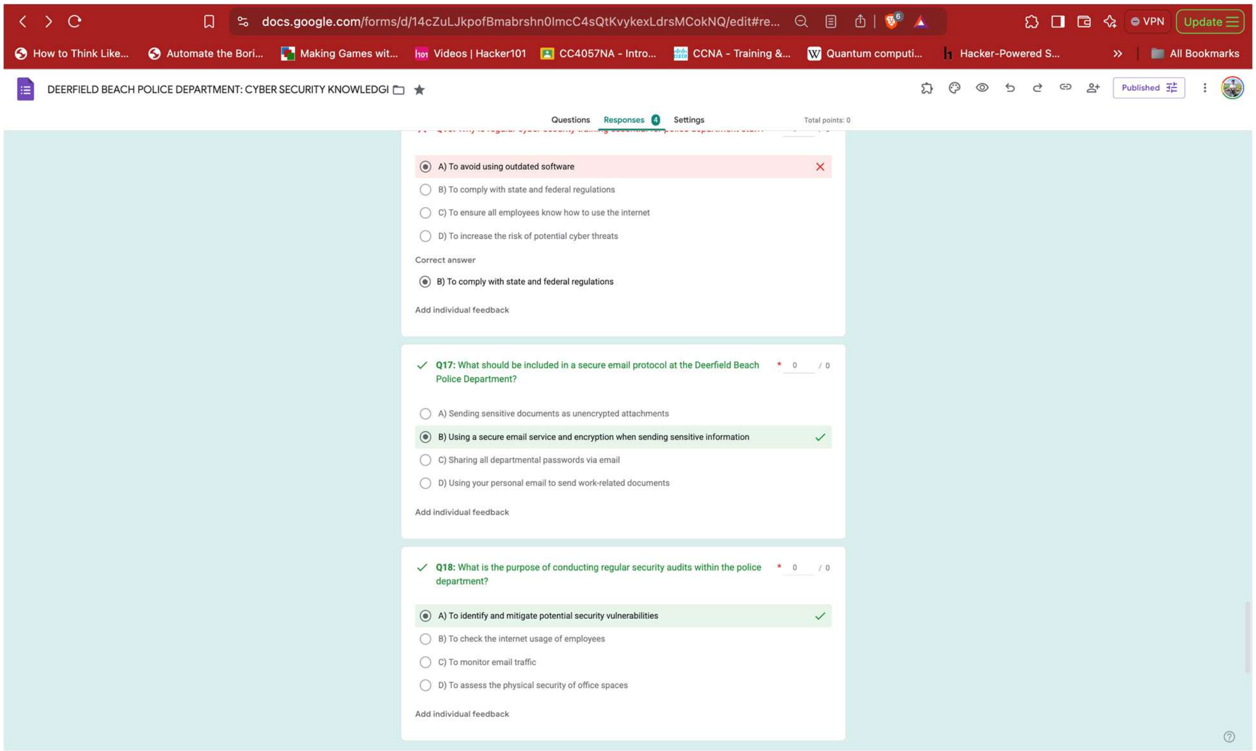
✗ **Q15:** What should you do with sensitive information you no longer need to access? * 0 / 0

● A) Delete it without any further action ✗

○ B) Shred physical copies and securely delete digital files

○ C) Store it on your local hard drive

○ D) Leave it in your inbox for future reference



● A) To avoid using outdated software ✗

○ B) To comply with state and federal regulations

○ C) To ensure all employees know how to use the internet

○ D) To increase the risk of potential cyber threats

Correct answer

● B) To comply with state and federal regulations

Add individual feedback

✓ **Q17:** What should be included in a secure email protocol at the Deerfield Beach Police Department? * 0 / 0

○ A) Sending sensitive documents as unencrypted attachments

● B) Using a secure email service and encryption when sending sensitive information ✓

○ C) Sharing all departmental passwords via email

○ D) Using your personal email to send work-related documents

Add individual feedback

✓ **Q18:** What is the purpose of conducting regular security audits within the police department? * 0 / 0

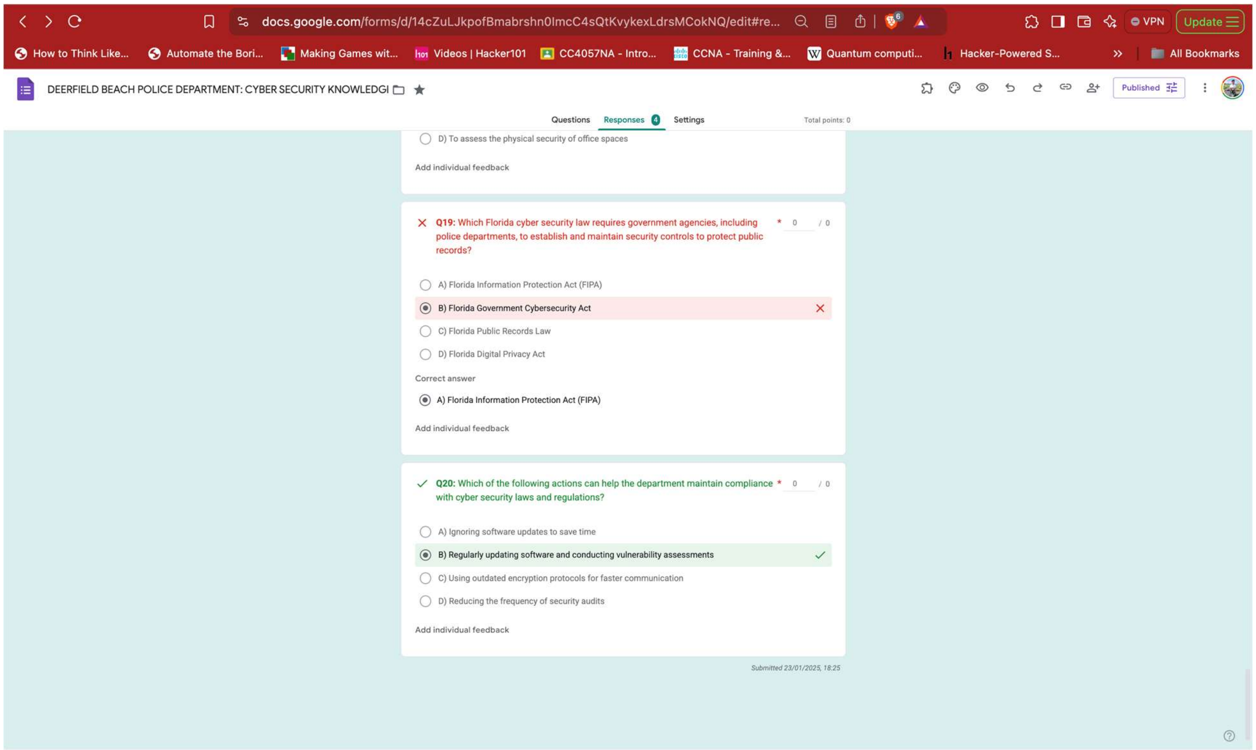
● A) To identify and mitigate potential security vulnerabilities ✓

○ B) To check the internet usage of employees

○ C) To monitor email traffic

○ D) To assess the physical security of office spaces

Add individual feedback



○ D) To assess the physical security of office spaces

Add individual feedback

✗ **Q19:** Which Florida cyber security law requires government agencies, including police departments, to establish and maintain security controls to protect public records? * 0 / 0

○ A) Florida Information Protection Act (FIPA)

● B) Florida Government Cybersecurity Act ✗

○ C) Florida Public Records Law

○ D) Florida Digital Privacy Act

Correct answer

● A) Florida Information Protection Act (FIPA)

Add individual feedback

✓ **Q20:** Which of the following actions can help the department maintain compliance with cyber security laws and regulations? * 0 / 0

○ A) Ignoring software updates to save time

● B) Regularly updating software and conducting vulnerability assessments ✓

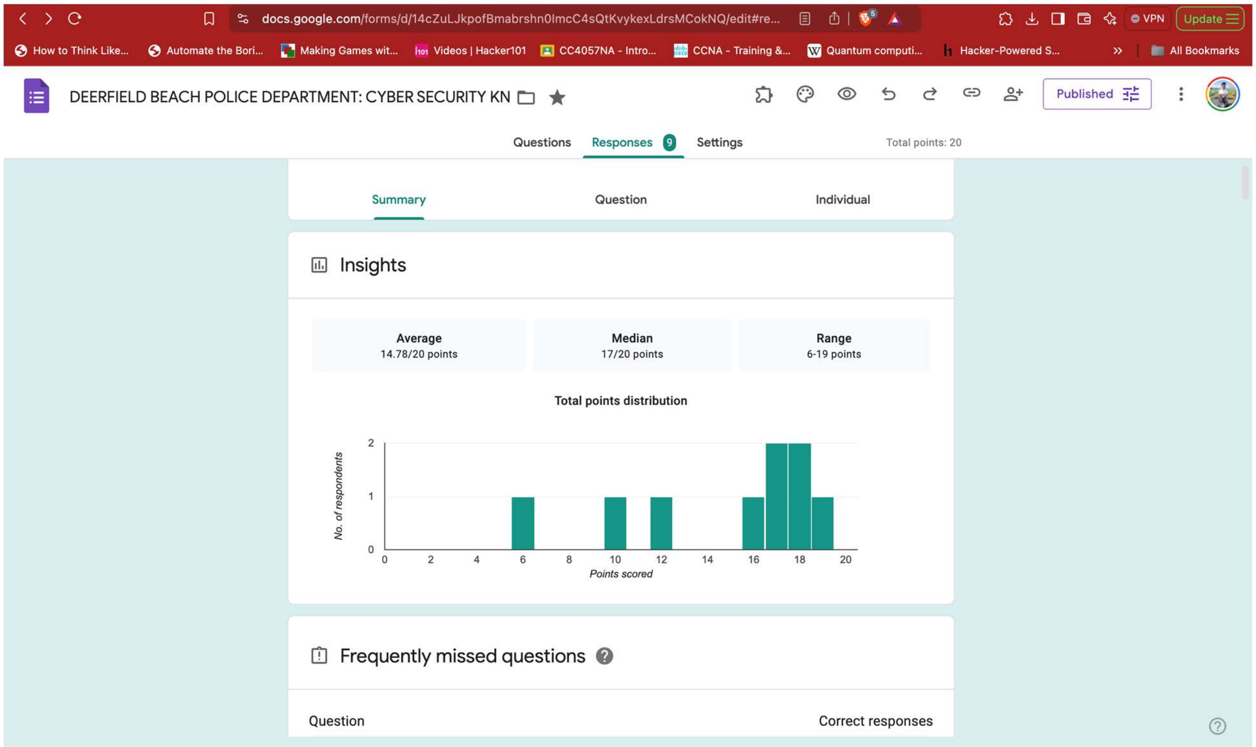
○ C) Using outdated encryption protocols for faster communication

○ D) Reducing the frequency of security audits

Add individual feedback

Submitted 23/01/2025, 18:25

Data Insights



DEERFIELD BEACH POLICE DEPARTMENT: CYBER SECURITY KN

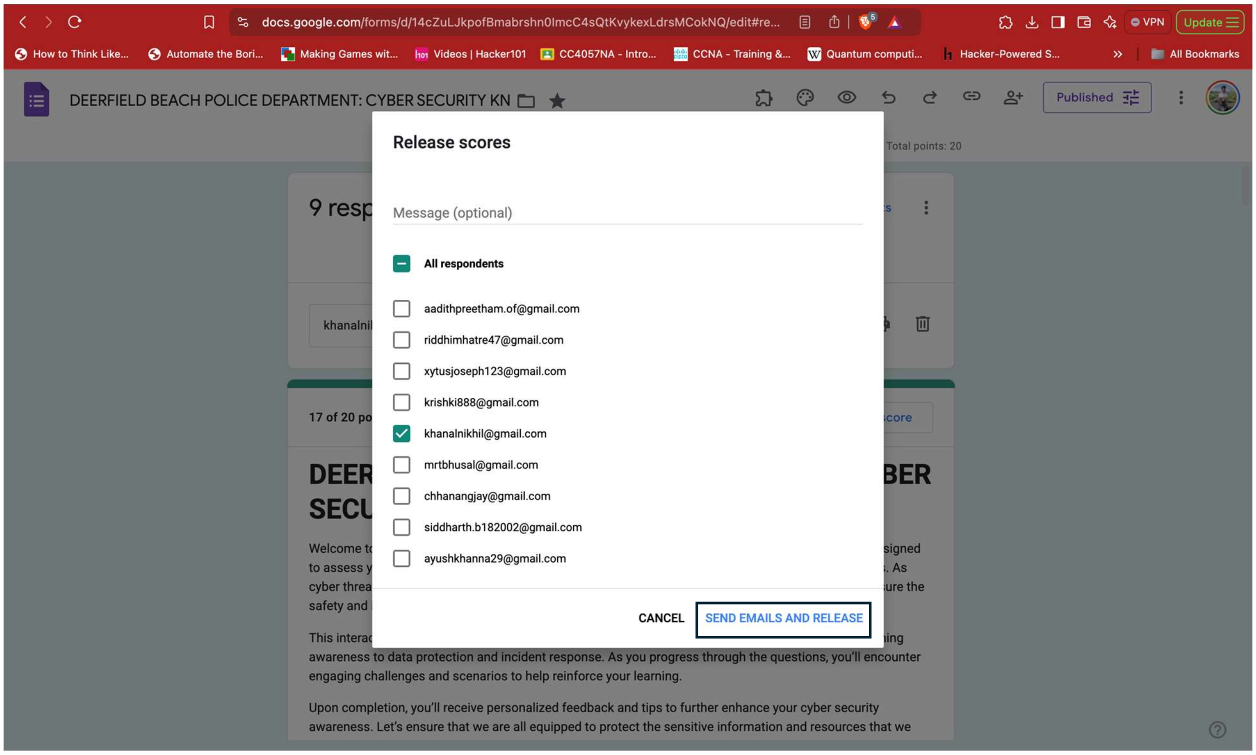
Total points: 20

Average	Median	Range
14.78/20 points	17/20 points	6-19 points

Question	Correct responses

Insights on response can be seen on chart format. As the data here shows score, number of responses, once the survey is done an email notification will be sent to everyone informing them about their results and score.

Score release Demo


docs.google.com/forms/d/14cZuLJkpofBmabrshn0lmcC4sQtKvykexLdrsMCokNQ/edit#re...
VPN
Update
How to Think Like...
Automate the Bori...
Making Games wit...
Videos | Hacker101
CC4057NA - Intro...
CCNA - Training &...
Quantum computi...
Hacker-Powered S...
All Bookmarks
DEERFIELD BEACH POLICE DEPARTMENT: CYBER SECURITY KN
Published
Total points: 20
9 resp
khanalni
17 of 20 po
score
DEER
SECU
BER
Welcome t
to assess y
cyber threa
safety and
signed
. As
ure the
This interac
ing
awareness to data protection and incident response. As you progress through the questions, you'll encounter engaging challenges and scenarios to help reinforce your learning.
Upon completion, you'll receive personalized feedback and tips to further enhance your cyber security awareness. Let's ensure that we are all equipped to protect the sensitive information and resources that we

Release scores

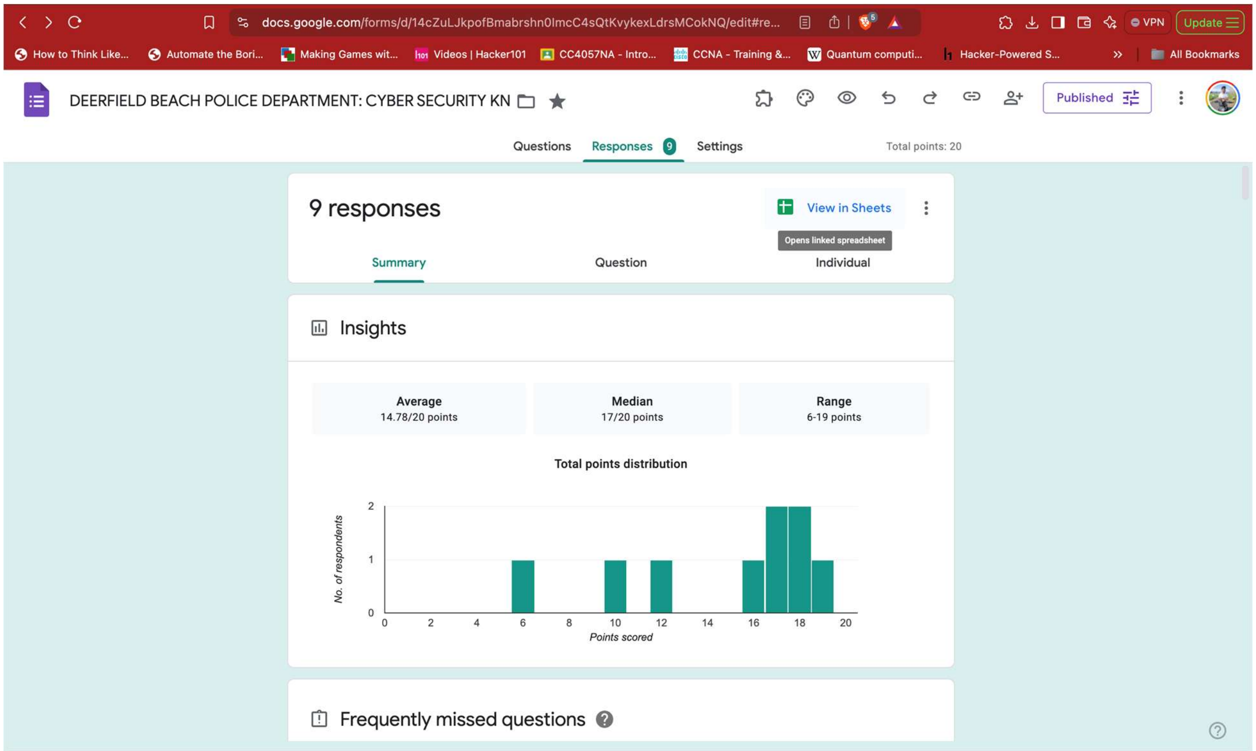
Message (optional)

⊟ **All respondents**

☐ aadithpreetham.of@gmail.com
☐ riddhimhatre47@gmail.com
☐ xytusjoseph123@gmail.com
☐ krishki888@gmail.com
☑ khanalnikhil@gmail.com
☐ mrtbhusal@gmail.com
☐ chhanangjay@gmail.com
☐ siddharth.b182002@gmail.com
☐ ayushkhanna29@gmail.com

CANCEL
SEND EMAILS AND RELEASE

The score can be release to either individual or as a whole group. After the score is released an email notification is send to users to check for their score.


docs.google.com/forms/d/14cZuLJkpofBmabrshn0lmcC4sQtKvykexLdrsMCokNQ/edit#re...
How to Think Like... | Automate the Bori... | Making Games wit... | Videos | Hacker101 | CC4057NA - Intro... | CCNA - Training &... | Quantum computi... | Hacker-Powered S... | All Bookmarks
VPN
Update
Published
Questions
Responses 9
Settings
Opens linked spreadsheet
View in Sheets
Summary
Question
Individual
2
1
0
No. of respondents
0
2
4
6
8
10
12
14
16
18
20
Points scored

DEERFIELD BEACH POLICE DEPARTMENT: CYBER SECURITY KN

Total points: 20

9 responses

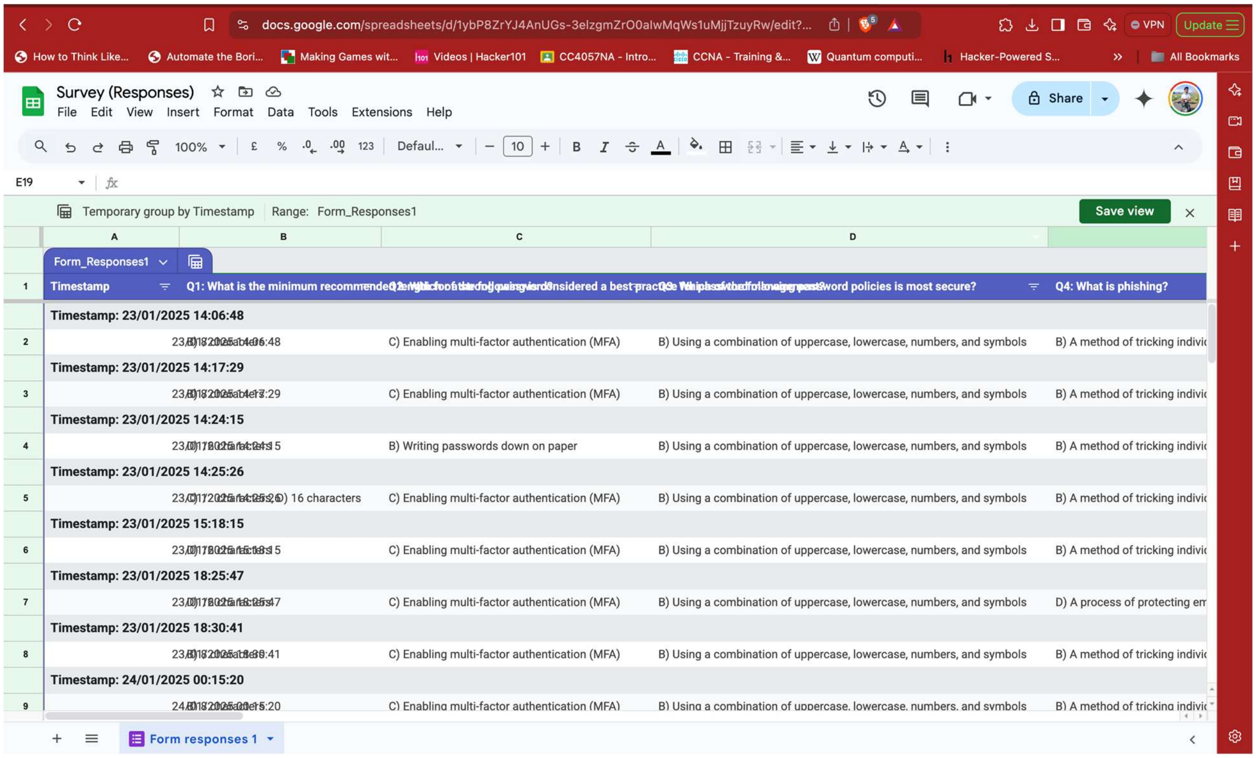
Insights

Average	Median	Range
14.78/20 points	17/20 points	6-19 points

Total points distribution

Frequently missed questions

The survey responses are linked in sheets and can be viewed as below.


docs.google.com/spreadsheets/d/1ybP8ZrYJ4AnUGs-3elzgmZrO0alwMqWs1uMjTzuyRw/edit?...
How to Think Like... | Automate the Bori... | Making Games wit... | Videos | Hacker101 | CC4057NA - Intro... | CCNA - Training &... | Quantum computi... | Hacker-Powered S... | All Bookmarks
VPN
Update
File Edit View Insert Format Data Tools Extensions Help
Share
100%
£ % .0 .00 123
Defaul...
10
B I
E19
Save view
Form responses 1

Survey (Responses)

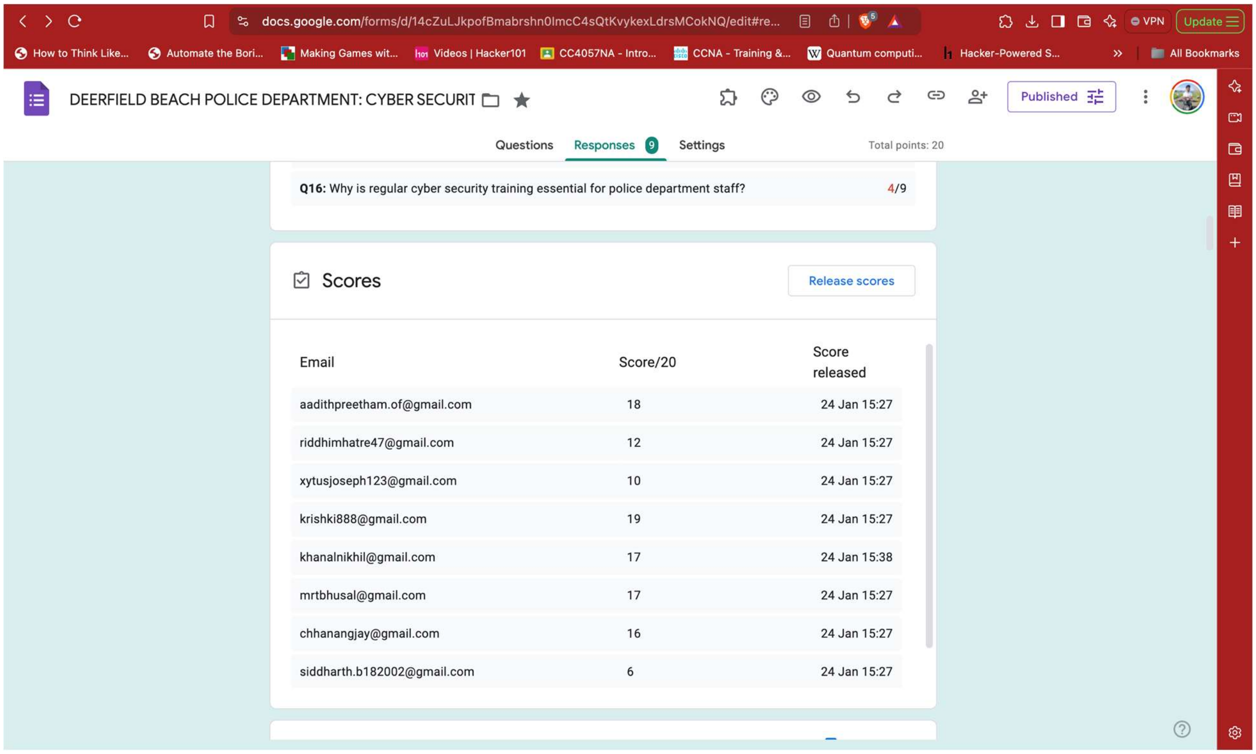
Temporary group by Timestamp Range: Form_Responses1

Form_Responses1

	A	B	C	D	
1	Timestamp	Q1: What is the minimum recommende	Q2: Which of the following is considered a best practice	Q3: Which of the following password policies is most secure?	Q4: What is phishing?
	Timestamp: 23/01/2025 14:06:48				
2	23/B)18 2025a14e06:48		C) Enabling multi-factor authentication (MFA)	B) Using a combination of uppercase, lowercase, numbers, and symbols	B) A method of tricking indivic
	Timestamp: 23/01/2025 14:17:29				
3	23/B)18 2025a14e17:29		C) Enabling multi-factor authentication (MFA)	B) Using a combination of uppercase, lowercase, numbers, and symbols	B) A method of tricking indivic
	Timestamp: 23/01/2025 14:24:15				
4	23/D)17 2025 14:24:15		B) Writing passwords down on paper	B) Using a combination of uppercase, lowercase, numbers, and symbols	B) A method of tricking indivic
	Timestamp: 23/01/2025 14:25:26				
5	23/C)17 2025 14:25:26	D) 16 characters	C) Enabling multi-factor authentication (MFA)	B) Using a combination of uppercase, lowercase, numbers, and symbols	B) A method of tricking indivic
	Timestamp: 23/01/2025 15:18:15				
6	23/D)17 2025 15:18:15		C) Enabling multi-factor authentication (MFA)	B) Using a combination of uppercase, lowercase, numbers, and symbols	B) A method of tricking indivic
	Timestamp: 23/01/2025 18:25:47				
7	23/D)17 2025 18:25:47		C) Enabling multi-factor authentication (MFA)	B) Using a combination of uppercase, lowercase, numbers, and symbols	D) A process of protecting em
	Timestamp: 23/01/2025 18:30:41				
8	23/B)18 2025a18e30:41		C) Enabling multi-factor authentication (MFA)	B) Using a combination of uppercase, lowercase, numbers, and symbols	B) A method of tricking indivic
	Timestamp: 24/01/2025 00:15:20				
9	24/B)18 2025a00e15:20		C) Enabling multi-factor authentication (MFA)	B) Using a combination of uppercase, lowercase, numbers, and symbols	B) A method of tricking indivic

Leaderboard

After the score is released, the leaderboard is maintained automatically in google forms which sorts the employees and staffs as their scores in ascending order from highest to lowest.



DEERFIELD BEACH POLICE DEPARTMENT: CYBER SECURIT

Q16: Why is regular cyber security training essential for police department staff? 4/9

Scores

Email	Score/20	Score released
aadithpreetham.of@gmail.com	18	24 Jan 15:27
riddhimhatre47@gmail.com	12	24 Jan 15:27
xytusjoseph123@gmail.com	10	24 Jan 15:27
krishki888@gmail.com	19	24 Jan 15:27
khanalnikhil@gmail.com	17	24 Jan 15:38
mrtbhusal@gmail.com	17	24 Jan 15:27
chhanangjay@gmail.com	16	24 Jan 15:27
siddharth.b182002@gmail.com	6	24 Jan 15:27

Conclusion

In conclusion, this initiative has not only met its primary objective of assessing staff knowledge, engaging them but has also paved the way for ongoing learning and improvement in the department's overall approach to cyber security.