Section Quiz

Candidate: Dunkan Gibson (dunkan.gibson)
Date: 2/24/2022 7:51:04 pm • Time spent: 00:09

Score: 0% Passing Score: 80%

Question 1: ✕ Incorrect

You are investigating the use of website and URL content filtering to prevent users from visiting certain websites.

Which benefits are the result of implementing this technology in your organization? (Choose two.)

- [ ] Prevention of phishing attempts
- [ ] An increase in bandwidth availability
- [ ] Enforcement of the organization's internet usage policy
- [ ] Prevention of emails containing threats
- [ ] Identification and disposal of infected content

EXPLANATION

Website filtering can be used to enforce the organization's internet usage policy and usually results in an increase in bandwidth availability.

Spam blockers are used to block emails containing threats. Virus blockers identify infected content and dispose of it. Anti-phishing software scans content to identify and dispose of phishing attempts, preventing outside attempts to access confidential information.

REFERENCES

5.6.4 Web Threat Protection Facts

q_web_threat_prot_content_secp7.question.fex

Question 2: ✕ Incorrect

Travis is sending a highly confidential email to Craig that contains sensitive data. Which of the following should Travis implement to ensure that only Craig is able to read the email?

- Virus scanner
- Encryption
- Anti-phishing software
- Spam filter

EXPLANATION

Encryption causes data, such as the content of an email, to be unintelligible except to those who have the proper key to decrypt it. Travis should make sure to encrypt the email before sending it so that only Craig is able to open the email and read the contents.

Virus scanners identify infected content and dispose of it.

Gateway email spam filters prevent spam emails from reaching your network, servers, and computers.

Anti-phishing software scans content to identify and dispose of phishing attempts, preventing outside attempts to access confidential information.

REFERENCES

5.6.4 Web Threat Protection Facts

q_web_threat_prot_encryption_secp7.question.fex

Question 3: ✕ Incorrect

Which of the following types of proxies would you use to remain anonymous when surfing the internet?

- Reverse
- Forward
- Content filter
- VPN

EXPLANATION

Forward proxies can be used to filter web content but can also be used to mask a user's identity for anonymity.

Reverse proxies can be used for caching and authentication.

Content filtering is not a type of proxy server.

A VPN is not a type of proxy and is not used for web filtering.

REFERENCES

5.6.4 Web Threat Protection Facts

q_web_threat_prot_forward_secp7.question.fex

Question 4: ✕ Incorrect

As the security analyst for your organization, you have noticed an increase in emails that attempt to trick users into revealing confidential information. Which web threat solution should you implement to protect against these threats?

- Data loss prevention
- Anti-phishing software
- Proxies
- Encryption

EXPLANATION

Anti-phishing software scans content to identify and dispose of phishing attempts, preventing outside attempts to access confidential information.

Proxies are used to filter web content and protect users on the internet. This would not help against phishing attempts.

Data loss prevention are types of software that protect sensitive data from being exposed. This would not help against phishing attempts.

Encryption causes data, such as the content of an email, to be unintelligible except to those who have the proper key to decrypt it. This would not help against phishing attempts.

REFERENCES

- 1.2.3 Defense Planning Facts
- 2.3.1 Social Engineering Overview
- 2.3.2 Social Engineering Overview Facts
- 2.3.3 Social Engineering Motivation
- 2.3.4 Social Engineering Motivation Facts
- 2.3.5 Social Engineering Techniques
- 2.3.6 Social Engineering Techniques Facts
- 2.3.7 Phishing and Internet-Based Techniques
- 2.3.8 Phishing and Internet-Based Techniques Facts
- 2.3.9 Use the Social Engineer Toolkit
- 2.3.10 Investigating a Social Engineering Attack
- 2.3.11 Identify Social Engineering

5.6.4 Web Threat Protection Facts

13.3.2 Email Security Facts

q_web_threat_prot_phishing_secp7.question.fex

Question 5: ✕ Incorrect

Which of the following are functions of gateway email spam filters? (Select two.)

- [x] Filters messages containing specific content
- [x] Blocks email from specific senders
- [ ] Blocks users from visiting websites with malicious content
- [ ] Helps enforce an organization's internet usage policy
- [ ] Blocks phishing attempts, which try to access confidential information

EXPLANATION

Gateway email spam filters can be used to block the following:

- Messages from specific senders
- Email containing threats (such as false links)
- Messages containing specific content

Web threat filtering prevents users from visiting websites with known malicious content. Website and content filtering can be used to enforce the organization's internet usage policy. Anti-phishing software scans content to identify and dispose of phishing attempts, preventing outsiders from accessing confidential information.

REFERENCES

2.3.1 Social Engineering Overview

2.3.2 Social Engineering Overview Facts

2.3.3 Social Engineering Motivation

2.3.4 Social Engineering Motivation Facts

2.3.5 Social Engineering Techniques

2.3.6 Social Engineering Techniques Facts

2.3.7 Phishing and Internet-Based Techniques

2.3.8 Phishing and Internet-Based Techniques Facts

2.3.9 Use the Social Engineer Toolkit

2.3.10 Investigating a Social Engineering Attack

2.3.11 Identify Social Engineering

5.6.1 Web Threat Protection

5.6.4 Web Threat Protection Facts

13.3.2 Email Security Facts

13.3.3 Protecting a Client from Spam

q_web_threat_prot_spam_01_secp7.question.fex

Question 6: ✕ Incorrect

You are configuring web threat protection on the network and want to block emails coming from a specific sender. Which of the following should be configured?

- Anti-phishing software
- Spam filter
- Encryption
- Virus scanner

EXPLANATION

Gateway email spam filters prevent spam emails from reaching your network, servers, and computers. Spam filters can be configured to block specific senders, emails containing threats (such as false links), and emails containing specific content. Content filtering can block users from visiting specific categories of websites.

Virus scanners identify infected content and dispose of it.

Encryption causes data, such as the content of an email, to be unintelligible except to those who have the proper key to decrypt it.

Anti-phishing software scans content to identify and dispose of phishing attempts, preventing outside attempts to access confidential information.

REFERENCES

5.6.4 Web Threat Protection Facts

q_web_threat_prot_spam_02_secp7.question.fex

Question 7: ✕ Incorrect

As the security analyst for your organization, you have noticed an increase in user computers being infected with malware. Which two solutions should you implement and configure to remedy this problem? (Select two.)

- [ ] Data loss prevention
- [ ] Proxies
- [ ] Encryption
- [x] Virus scanner
- [x] Spam filters

EXPLANATION

Virus scanners identify infected content and dispose of it. They are often coupled with email scanners. Gateway email spam filters prevent spam emails from reaching your network, servers, and computers. Since the most likely cause of malware infections is through spam emails, implementing spam filters and virus scanners helps remedy the problem.

Proxies are used to filter web content and protect users on the internet. This would not help remedy malware issues.

Data loss prevention are types of software that protect sensitive data from being exposed. This would not help remedy malware issues.

Encryption causes data, such as the content of an email, to be unintelligible except to those who have the proper key to decrypt it. This would not help remedy malware issues.

REFERENCES

2.3.1 Social Engineering Overview

2.3.2 Social Engineering Overview Facts

2.3.3 Social Engineering Motivation

2.3.4 Social Engineering Motivation Facts

2.3.5 Social Engineering Techniques

2.3.6 Social Engineering Techniques Facts

2.3.7 Phishing and Internet-Based Techniques

2.3.8 Phishing and Internet-Based Techniques Facts

2.3.9 Use the Social Engineer Toolkit

2.3.10 Investigating a Social Engineering Attack

2.3.11 Identify Social Engineering

5.6.1 Web Threat Protection

5.6.4 Web Threat Protection Facts

13.3.2 Email Security Facts

13.3.3 Protecting a Client from Spam

q_web_threat_prot_spam_03_secp7.question.fex

Question 8: ✕ Incorrect

You are configuring web threat protection on the network and want to prevent users from visiting www.videosite.org. Which of the following needs to be configured?

- Content filtering
- Virus scanner
- ➡ Website filtering
- Anti-phishing software

EXPLANATION

To block users from visiting a specific site, you should configure website filtering.

Content filtering can block users from visiting specific categories of websites.

Virus scanners identify infected content and dispose of it.

Anti-phishing software scans content to identify and dispose of phishing attempts, preventing outside attempts to access confidential information.

REFERENCES

5.6.4 Web Threat Protection Facts

q_web_threat_prot_url_filter_secp7.question.fex

Question 9: ✕ Incorrect

Which of the following types of proxies can be used for web filtering?

- Reverse
- Content filter
- VPN
- ➡ Transparent

EXPLANATION

Transparent proxies are located between a user and the internet, and they can redirect requests without changing them. These can also be used for web filtering.

Reverse proxies can be used for caching and authentication.

A VPN is not a type of proxy and is not used for web filtering.

Content filtering is not a type of proxy server.

REFERENCES

5.6.4 Web Threat Protection Facts

q_web_threat_prot_web_filter_secp7.question.fex

Question 10: ✕ Incorrect

You are configuring web threat protection on the network and have identified a website that contains malicious content. Which of the following should you configure?

- ➡ Web threat filtering
- Content filtering
- Anti-phishing software
- Virus scanner

EXPLANATION

Web threat filtering prevents a user from visiting websites with known malicious content. An administrator can monitor sites that have become infected with spyware or other malware and add them to the list of blocked sites.

Content filtering can block users from visiting specific categories of websites.

Virus scanners identify infected content and dispose of it.

Anti-phishing software scans content to identify and dispose of phishing attempts, preventing outside attempts to access confidential information.

REFERENCES

5.6.4 Web Threat Protection Facts

q_web_threat_prot_web_threat_secp7.question.fex