200 XP

Summary and knowledge check

5 minutes

Microsoft Defender for Office 365 provides protection against some of the most common organizational attacks, ranging from malicious attachments to harmful redirected links contained in the body of an email. By providing robust zero-day protection, and featuring the rich reporting and URL trace capabilities, security administrators have real-time insights into the attacks happening in your organization.

Check your knowledge

1. What are two of the most common phishing attacks made on an organization?

- ○ Distributed denial of service (DDoS) and spam
- ○ Malicious attachments and DDoS
- ○ Spam and malicious hyperlinks
- ○ Malicious attachments and hyperlinks

2. The Contoso organization has Office 365 Enterprise E5 for all users. The security administrator has defined specific anti-phishing policies for the finance department but hasn't applied those policies elsewhere. Which of the following is true?

- ○ Microsoft Defender for Office 365 anti-phishing protection is in place for all of Contoso
- ○ Microsoft Defender for Office 365 advanced anti-phishing protection is in place for finance, while all other Contoso users receive baseline anti-phishing protection.
- ○ Microsoft Defender for Office 365 anti-phishing protection is in place for finance and all newly created users, but not for the rest of Contoso.
- ○ Microsoft Defender for Office 365 anti-phishing protection is in place for only the finance department.

3. What anti-phishing policy option should be used to ensure an outside attacker can’t impersonate the CEO of your organization?

- ○ Add impersonation policy

- ○ Add users to protect
- ○ Add trusted senders and domains
- ○ Add domains to protect

Check your answers