Nama: _____ Tanggal: _____ Nilai: _____

Serangan Phishing & Rekayasa Sosial

Spear phishing, penipuan whaling, protokol SPF/DKIM/DMARC, spoofing pengirim, dan pelatihan keamanan karyawan.

GAMBARAN PEMBELAJARAN SERANGAN PHISHING

TERAMANKAN
ENKRIPSI DATA
Standar AES 256-bit

PATUH
STANDAR GLOBAL
Kerangka GDPR & CCPA

ZERO TRUST
KEBIJAKAN AKSES
Autentikasi Multifaktor

Selamat datang! Paket aktivitas ini memandu Anda mempelajari serangan phishing dan rekayasa sosial. Anda akan mempelajari spear phishing, whaling, pemalsuan domain, protokol SPF/DKIM/DMARC, keamanan tautan, dan pelatihan kesadaran karyawan.

POS-POS LEMBAR KERJA

- [ ] **Bagian 1-4: Kuasai keamanan siber dan pencegahan ancaman.**
- [ ] **Bagian 5-7: Selesaikan teka-teki silang & pencarian kata.**
- [ ] **Bagian 8-9: Selesaikan studi kasus & tantangan sandi.**
- [ ] **Bagian 10: Pelajari halaman FAQ dasar & lanjutan.**
- [ ] **Bagian 11: Jelajahi 10 fakta menarik dari dunia nyata.**
- [ ] **Bonus: Tantangan Berpikir Cepat.**

Buka Panduan Keamanan Siber VPN.com

URL: https://www.vpn.com/cybersecurity/phishing-attacks/

Peta Belajar Mitigasi Phishing Anda

- Kenali phishing, vishing, dan penipuan pop-up dukungan teknis yang umum.
- Terapkan prosedur verifikasi transaksi di luar kanal.
- Atur aturan SPF, DKIM, dan DMARC untuk memblokir domain tiruan.

PETUNJUK PANDUAN SERANGAN PHISHING

Jawab soal pilihan ganda dan benar/salah, lengkapi kalimat rumpang dengan bank kata, cocokkan definisi, serta selesaikan teka-teki silang dan pencarian kata. Terapkan pengetahuan Anda tentang autentikasi email. Akhiri dengan aktivitas bonus Berpikir Cepat.

SERANGAN PHISHING & REKAYASA SOSIAL (PENGANTAR)

Serangan phishing memakai pesan terarah, penipuan whaling, dan pemalsuan domain untuk mengumpulkan kredensial login pengguna. Mengamankan sistem perusahaan memerlukan aturan SPF, DKIM, dan DMARC di gerbang serta langkah persetujuan di luar kanal.

BACA SETIAP POS DENGAN SAKSAMA DAN PILIH ATAU TULIS JAWABAN YANG BENAR.

Pos 1: Tantangan Pilihan Ganda

1 **1. Apa itu spear phishing?**

- A. Email phishing terarah yang disesuaikan untuk orang atau organisasi tertentu
- B. Email massal ke jutaan alamat acak
- C. Serangan jaringan yang membanjiri server web
- D. Teknik pengambilan data pengguna dari basis data

2 **2. Protokol mana yang memungkinkan domain mencantumkan alamat IP pengirim resminya di DNS untuk melawan spoofing?**

- A. SPF
- B. DKIM
- C. DMARC
- D. HTTPS

3 **3. Apa itu serangan whaling?**

- A. Kampanye phishing yang khusus mengincar eksekutif perusahaan ternama
- B. Serangan injeksi SQL terhadap cadangan basis data
- C. Pencurian fisik perangkat router jaringan lokal
- D. Pemindaian brute-force credential stuffing otomatis

4 **4. Apa fungsi DKIM?**

- A. Menambahkan tanda tangan kriptografis untuk memverifikasi pengirim
- B. Memblokir paket masuk di firewall
- C. Mengenkripsi volume penyimpanan basis data
- D. Memindai lampiran email untuk malware

5 **5. Apa peran DMARC?**

- A. Mengarahkan server penerima cara menangani email yang gagal cek SPF/DKIM
- B. Membongkar kata sandi dengan rainbow table
- C. Mengompresi lampiran email sebelum dikirim
- D. Mengatur hak akses perutean jaringan

Pos 2: Tantangan Benar atau Salah

6 Pertanyaan 6

6. Spear phishing mengandalkan email massal umum ke jutaan alamat acak.

Benar Salah

7 Pertanyaan 7

7. Kebijakan DMARC dapat memerintahkan server email menolak pesan tiruan.

Benar Salah

8 Pertanyaan 8

8. Verifikasi SPF bekerja dengan memvalidasi tanda tangan kriptografis isi email.

Benar Salah

9 Pertanyaan 9

9. Serangan whaling mengincar administrator tingkat bawah untuk mengakses berkas basis data.

Benar Salah

10 Pertanyaan 10

10. Verifikasi out-of-band atas permintaan pembayaran membantu menghentikan penipuan transfer dana.

Benar Salah

Pos 3: Mengisi Istilah Kunci

Baca setiap kalimat di bawah ini dan isi bagian yang kosong dengan istilah yang tepat dari Bank Kata.

1. Mengincar karyawan tertentu dengan informasi pribadi disebut _____ phishing.
2. Memalsukan header email agar pesan tampak asli disebut _____ .
3. Catatan DNS berisi daftar IP server email resmi adalah _____ .
4. Standar tanda tangan email untuk verifikasi pengirim adalah _____ .
5. Kebijakan untuk menolak email yang gagal cek SPF/DKIM memakai _____ .
6. Kampanye phishing yang mengincar eksekutif puncak disebut _____ .

BANK KATA KOSAKATA

DKIM DMARC PHISHING SPEAR SPF SPOOFING VISHING WHALING

Tulis jawaban Anda di sini:

1.
2.
3.
4.
5.
6.

Pos 4: Pencocokan Konsep Keamanan

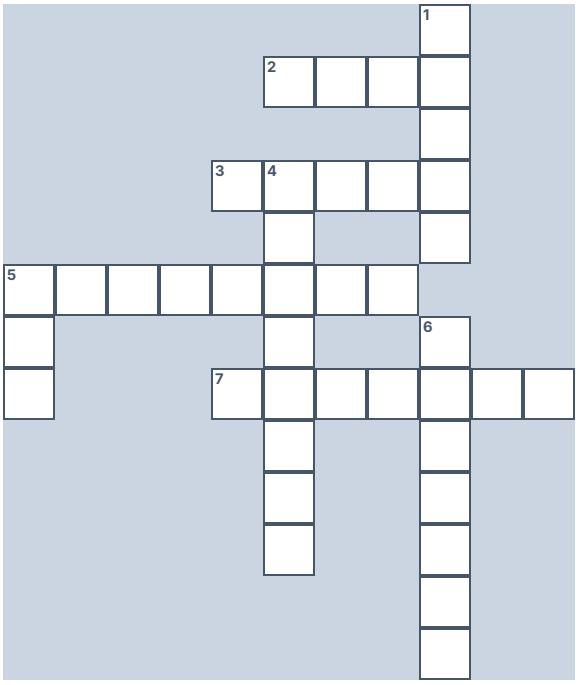
MENCOCOKKAN DEFINISI

Cocokkan setiap istilah di sebelah kiri dengan definisi yang benar di sebelah kanan dengan menulis huruf yang sesuai (A-H) di kotak isian.

☐	1. SPEAR	A	Panggilan penipuan lewat suara.
☐	2. SPOOFING	B	Mengincar eksekutif puncak.
☐	3. SPF	C	Instruksi kebijakan penolakan.
☐	4. DKIM	D	IP pengirim resmi di DNS.
☐	5. DMARC	E	Email rekayasa sosial.
☐	6. WHALING	F	Email terarah yang dipersonalisasi.
☐	7. PHISHING	G	Memalsukan alamat email pengirim.
☐	8. VISHING	H	Tanda tangan kriptografis di email.

Pos 5: Teka-Teki Silang

Selesaikan teka-teki silang dengan mengetik huruf di kotak putih yang aktif. Nomor-nomornya sesuai dengan petunjuk di bawah.



PETUNJUK MENDATAR

2. Standar yang menambahkan tanda tangan kriptografis ke email (4)

3. ... phishing: email terarah untuk orang tertentu (5)

5. Pemalsuan pengirim agar email tampak asli (8)

7. Phishing yang mengincar eksekutif puncak (7)

PETUNJUK MENURUN

1. Aturan yang memberi tahu server cara menangani email yang gagal SPF atau DKIM (5)

4. Pesan penipuan yang memancing pengguna membagikan data (8)

5. Catatan DNS berisi daftar server email resmi (3)

6. Penipuan lewat panggilan telepon (7)

Alternatif Pos 5: Petunjuk Teka-Teki Silang yang Aksesibel

Pengguna pembaca layar dan keyboard dapat mengetik jawaban teka-teki silang langsung di kolom teks di bawah ini.

PETUNJUK MENDATAR

2 mendatar: Standar yang menambahkan tanda tangan kriptografis ke email (4 huruf):

3 mendatar: ... phishing: email terarah untuk orang tertentu (5 huruf):

5 mendatar: Pemalsuan pengirim agar email tampak asli (8 huruf):

7 mendatar: Phishing yang mengincar eksekutif puncak (7 huruf):

PETUNJUK MENURUN

1 menurun: Aturan yang memberi tahu server cara menangani email yang gagal SPF atau DKIM (5 huruf):

4 menurun: Pesan penipuan yang memancing pengguna membagikan data (8 huruf):

5 menurun: Catatan DNS berisi daftar server email resmi (3 huruf):

6 menurun: Penipuan lewat panggilan telepon (7 huruf):

Pos 6: Mencari Kata Tersembunyi

Temukan 8 istilah kunci yang tersembunyi dalam kisi di bawah ini. Kata dapat tersusun mendatar, menurun, atau diagonal.

Y	P	X	F	P	L	C	S	R	I	G	N	R	M	P
X	Q	O	C	U	S	T	P	V	E	L	J	B	A	B
C	P	M	X	L	K	Y	E	K	I	X	T	K	D	Q
M	J	I	D	I	N	N	A	K	Q	S	P	G	M	M
Q	R	K	S	T	S	T	R	G	C	D	H	S	Q	O
G	H	D	S	B	P	W	P	D	S	Z	M	I	V	C
N	Z	W	F	K	O	H	Z	H	D	N	D	A	N	Q
I	X	P	C	U	O	B	A	Z	I	N	D	K	R	G
L	A	D	O	D	F	F	H	I	D	S	R	Q	M	C
A	E	I	R	Z	I	S	F	Q	V	F	H	A	A	Q
H	O	N	P	T	N	X	Q	K	R	U	S	I	D	N
W	Y	B	F	S	G	X	W	J	F	A	R	Z	N	Y
Y	L	G	I	M	R	J	M	P	L	T	O	H	Q	G
Q	H	Z	A	O	V	G	S	U	B	Y	R	Y	B	H
L	Z	G	J	O	P	N	W	C	M	Z	Y	G	Y	O

DAFTAR KOSAKATA

SPEAR SPOOFING SPF DKIM DMARC WHALING PHISHING VISHING

Alternatif Pos 6: Pencocokan Kosakata yang Aksesibel

Cocokkan kedelapan istilah dari Pencarian Kata dengan definisi yang benar dengan menulis hurufnya (A-H) di tempat kosong.

ISTILAH KOSAKATA
A. SPEAR
B. SPOOFING
C. SPF
D. DKIM
E. DMARC
F. WHALING
G. PHISHING
H. VISHING

DEFINISI & KOLOM PENCOCOKAN

1. Pemalsuan pengirim agar email tampak asli.
2. ... phishing: email terarah untuk orang tertentu.
3. Penipuan lewat panggilan telepon.
4. Catatan DNS berisi daftar server email resmi.
5. Pesan penipuan yang memancing pengguna membagikan data.
6. Aturan yang memberi tahu server cara menangani email yang gagal SPF atau DKIM.
7. Standar yang menambahkan tanda tangan kriptografis ke email.
8. Phishing yang mengincar eksekutif puncak.

Pos 7: Tantangan Kata Acak

Susun ulang huruf di bawah ini untuk menemukan konsep dan istilah kunci keamanan siber. Tulis jawaban Anda di kotak isian yang tersedia.

1. **AESRP** _____
2. **FPS** _____
3. **ADCRM** _____
4. **SNGIHPHI** _____
5. **FIPGOSNO** _____
6. **IMDK** _____
7. **WNIGHLA** _____
8. **IHGVNIS** _____

Aktivitas Bonus: Berpikir Cepat

3 JAWABAN UNTUK SETIAP KATEGORI. ORANG PERTAMA YANG MELENGKAPI DAFTAR MENANG.

1	Perangkat yang bisa diretas			
2	Tanda email phishing			
3	Tanda komputer terinfeksi			
4	Kata yang menciptakan desakan palsu			
5	Cara memeriksa pengirim			
6	Orang yang bisa dimintai bantuan TI			
7	Hal yang Anda cadangkan			
8	Ikan atau hewan laut yang Anda ketahui			
9	Perusahaan yang ditiru penipu			
10	Kebiasaan aman yang bisa dimulai hari ini			
11	Hal yang dilakukan setelah klik tautan palsu			
12	Hal yang dilakukan setelah kebocoran data			
13	Saluran tempat phishing terjadi			
14	Hal yang tidak pernah dikirim lewat email			
15	Cara melindungi akun Anda			

Pos 8: Studi Kasus Keamanan Siber

Terapkan konsep yang telah Anda pelajari untuk menyelesaikan skenario nyata di bawah ini.

STUDI KASUS 1: MENANGANI SERANGAN WHALING PADA EKSEKUTIF



Skenario: Seorang direktur keuangan menerima email yang sangat personal dan mengaku dari CEO, meminta transfer cepat $50.000 untuk menuntaskan pembelian domain rahasia.

Pertanyaan Diskusi: Analisis risiko peniruan merek, dan uraikan SPF/DKIM/DMARC serta kontrol autentikasi.

STUDI KASUS 2: MENERAPKAN KEBIJAKAN GERBANG SPF/DKIM/DMARC



Skenario: Sebuah perusahaan gagal audit keamanan karena email pemasarannya sering ditandai spam, dan peretas aktif memalsukan domain merek perusahaan.

Pertanyaan Diskusi: Susun kontrol teknis dan administratif untuk memverifikasi keaslian email.

Pos 9: Memecahkan Sandi

Seorang profesional keamanan siber melindungi aset jaringan dari pelaku ancaman online. Gunakan kunci Huruf-ke-Angka di bawah untuk memecahkan pesan dengan menulis huruf yang sesuai di tempat kosong.

KUNCI ENKRIPSI HURUF-KE-ANGKA

A=1 B=2 C=3 D=4 E=5 F=6 G=7 H=8 I=9 J=10 K=11 L=12 M=13

N=14 O=15 P=16 Q=17 R=18 S=19 T=20 U=21 V=22 W=23 X=24 Y=25 Z=26

16	5	18	9	11	19	1		16	5	14	7	9	18	9	13
19	**5**	**2**	**5**	**12**	**21**	**13**		**13**	**5**	**14**	**7**	**11**	**12**	**9**	**11**

Pesan yang dipecahkan:

TIPS: SETIAP ANGKA MEWAKILI POSISI HURUF TERSEBUT DALAM ALFABET (MISALNYA 1 = A, 2 = B, 26 = Z).

Pos 10: FAQ Dasar Keamanan Siber (Bagian A)

Pelajari pertanyaan dan jawaban umum tentang cara mengurangi ancaman online.

Q1: Apa itu phishing?

Phishing adalah serangan rekayasa sosial saat penjahat mengirim pesan penipuan agar pengguna membagikan data sensitif.

Q2: Apa beda phishing dan spear phishing?

Phishing mengincar kelompok luas dengan konten umum, sedangkan spear phishing mengincar korban tertentu dengan detail khusus.

Q3: Apa itu whaling?

Whaling adalah serangan phishing yang sangat terarah pada eksekutif ternama yang punya kewenangan administratif.

Q4: Apa itu email spoofing?

Email spoofing adalah pembuatan email dengan alamat pengirim palsu agar penerima memercayai sumbernya.

Q5: Bagaimana SPF mencegah pemalsuan?

SPF memuat daftar IP pengirim resmi di DNS, sehingga server penerima dapat memverifikasi sumber email. [1]

Pos 10: FAQ Dasar Keamanan Siber (Bagian B)

Pelajari pertanyaan dan jawaban umum tentang cara mengurangi ancaman online.

Q6: Apa itu DKIM?

DomainKeys Identified Mail menambahkan tanda tangan kriptografis ke header email, yang membuktikan bahwa sebuah domain bertanggung jawab atas pesan tersebut dan pesannya tidak diubah.

Q7: Apa kepanjangan DMARC?

Domain-based Message Authentication, Reporting, and Conformance. [2]

Q8: Apa itu kebijakan DMARC?

Kebijakan yang memberi tahu server email cara menangani pesan yang gagal SPF/DKIM (none, quarantine, atau reject). [2]

Q9: Apa itu vishing?

Phishing suara, saat penyerang memakai panggilan telepon palsu untuk mengorek data administratif atau keuangan.

Q10: Apa manfaat pemindai tautan?

Pemindai memeriksa dan menulis ulang tautan di email masuk untuk memastikan halaman tujuan aman saat diklik.

Pos 10: FAQ Lanjutan Keamanan (Bagian C)

Jelajahi aspek teknis lanjutan dari kerangka keamanan, analisis malware, dan kepatuhan data.

Q1: Bagaimana serangan homograf bekerja?

Penyerang mendaftarkan domain dengan karakter Unicode non-ASCII yang mirip agar tampak seperti domain asli.

Q2: Apa itu representasi punycode?

Pengodean yang mengubah nama domain Unicode menjadi string yang kompatibel dengan ASCII dan diawali 'xn--' agar dapat ditangani DNS.

Q3: Mengapa 'p=reject' adalah status DMARC paling aman?

Kebijakan ini meminta server penerima menolak email yang gagal DMARC (SPF/DKIM yang selaras) selama sesi SMTP, sehingga memblokir spoofing langsung. [2]

Q4: Bagaimana penyerang melewati aturan SPF?

Dengan memakai domain mirip (typosquatting) atau akun yang dibobol di layanan email pihak ketiga yang sah.

Q5: Apa itu business email compromise (BEC)?

Penipuan perusahaan saat penyerang membajak atau meniru akun email bisnis untuk menyetujui pembayaran palsu.

Pos 10: FAQ Lanjutan Keamanan (Bagian D)

Jelajahi aspek teknis lanjutan dari kerangka keamanan, analisis malware, dan kepatuhan data.

Q6: Bagaimana MFA menghentikan phishing?

MFA meminta token kedua (seperti kunci perangkat keras) yang tidak bisa dicuri lewat halaman tiruan saja.

Q7: Apa itu halaman pencuri kredensial?

Portal login tiruan yang menangkap nama pengguna, kata sandi, dan token MFA secara real time.

Q8: Apa itu pembajakan subdomain?

Penyerang mengambil alih subdomain DNS yang tidak dipakai untuk menampung halaman phishing di bawah domain induk tepercaya.

Q9: Bagaimana pemeriksaan kesesuaian DKIM bekerja?

Pemeriksaan ini memastikan domain di header 'From' sama dengan domain yang menandatangani pesan di header DKIM.

Q10: Apa peran gateway email?

Menyaring email masuk, memeriksa tautan, menguji lampiran di sandbox, dan memvalidasi kepatuhan SPF/DKIM/DMARC.

Bagian 11: 10 Fakta & Wawasan Keamanan Siber di Dunia Nyata

Pelajari fakta nyata tentang pelanggaran keamanan, mekanisme pertahanan, dan standar kepatuhan.

1. WAWASAN KEAMANAN

Phishing dan spoofing adalah jenis kejahatan yang paling banyak dilaporkan ke IC3 milik FBI pada 2025, dengan 191,561 pengaduan. [4]

2. WAWASAN KEAMANAN

Business email compromise (BEC) menyebabkan kerugian lebih dari $3 miliar yang dilaporkan ke IC3 milik FBI pada 2025. [4]

3. WAWASAN KEAMANAN

Serangan homograf memakai huruf Sirilik yang mirip untuk meniru domain merek di browser.

4. WAWASAN KEAMANAN

Dengan 'p=reject', sebuah domain meminta penerima menolak email yang gagal saat pengiriman, bukan menyimpannya sebagai spam. [2]

5. WAWASAN KEAMANAN

Serangan whaling terhadap CEO biasanya meminta pembayaran mendesak untuk merger atau pembelian domain rahasia.

6. WAWASAN KEAMANAN

Portal pemanenan kredensial meniru halaman login asli sehingga korban mengetik kata sandi langsung ke formulir milik penyerang.

7. WAWASAN KEAMANAN

Panduan phishing bersama dari CISA merekomendasikan pelatihan pengguna di samping DMARC, SPF, DKIM, dan MFA yang tahan phishing. [3]

8. WAWASAN KEAMANAN

Evaluasi SPF dibatasi hingga 10 term yang melakukan kueri DNS; melebihi batas ini menghasilkan hasil 'permerror'. [1]

9. WAWASAN KEAMANAN

Kunci keamanan perangkat keras FIDO2 memberi perlindungan kriptografis dari pencurian kredensial jarak jauh.

10. WAWASAN KEAMANAN

Phishing adalah salah satu cara paling umum penyerang pertama kali masuk ke sebuah organisasi, sehingga pelatihan kesadaran rutin menjadi pertahanan yang efektif.

Referensi & Sumber Teknis

Panduan belajar dan teka-teki interaktif ini disusun berdasarkan standar global NIST, OWASP, dan kepatuhan privasi data.

REFERENSI AKADEMIK & INDUSTRI

[1] IETF. (2014). RFC 7208: Sender Policy Framework (SPF) for Authorizing Use of Domains in Email, Version 1.

https://www.rfc-editor.org/rfc/rfc7208.html

[2] IETF. (2015). RFC 7489: Domain-based Message Authentication, Reporting, and Conformance (DMARC).

https://www.rfc-editor.org/rfc/rfc7489.html

[3] CISA. (2023). Phishing Guidance: Stopping the Attack Cycle at Phase One.

https://www.cisa.gov/resources-tools/resources/phishing-guidance-stopping-attack-cycle-phase-one

[4] FBI Internet Crime Complaint Center. (2026). 2025 IC3 Annual Report.

https://www.ic3.gov/AnnualReport/Reports/2025_IC3Report.pdf

[5] CISA. (n.d.). Malware, Phishing, and Ransomware.

https://www.cisa.gov/topics/cyber-threats-and-advisories/malware-phishing-and-ransomware

Kunci Jawaban: Pos 1 - Pilihan Ganda

1 Soal 1 — **Jawaban Benar: A**

CATATAN PENGAJAR

Apa itu spear phishing? → Email phishing terarah yang disesuaikan untuk orang atau organisasi tertentu

2 Soal 2 — **Jawaban Benar: A**

CATATAN PENGAJAR

SPF memublikasikan host pengirim resmi suatu domain di DNS agar penerima dapat memeriksa pengirim envelope.

3 Soal 3 — **Jawaban Benar: A**

CATATAN PENGAJAR

Apa itu serangan whaling? → Kampanye phishing yang khusus mengincar eksekutif perusahaan ternama

4 Soal 4 — **Jawaban Benar: A**

CATATAN PENGAJAR

Apa fungsi DKIM? → Menambahkan tanda tangan kriptografis untuk memverifikasi pengirim

5 Soal 5 — **Jawaban Benar: A**

CATATAN PENGAJAR

Apa peran DMARC? → Mengarahkan server penerima cara menangani email yang gagal cek SPF/DKIM

Kunci Jawaban: Pos 2 - Benar atau Salah

6 Soal 6

Jawaban Benar: Salah

CATATAN PENGAJAR

Salah: spear phishing disesuaikan untuk orang tertentu, berbeda dengan phishing massal yang umum.

7 Soal 7

Jawaban Benar: Benar

CATATAN PENGAJAR

Kebijakan DMARC dapat memerintahkan server email menolak pesan tiruan.

8 Soal 8

Jawaban Benar: Salah

CATATAN PENGAJAR

Salah: SPF mencocokkan IP pengirim dengan DNS; DKIM-lah yang memverifikasi tanda tangan kriptografis.

9 Soal 9

Jawaban Benar: Salah

CATATAN PENGAJAR

Salah: whaling menyasar eksekutif senior, yang dapat menyetujui pembayaran dan mengakses data sensitif.

10 Soal 10

Jawaban Benar: Benar

CATATAN PENGAJAR

Benar: mengonfirmasi permintaan pembayaran melalui saluran terpisah yang sudah dikenal membantu menghentikan penipuan transfer dana.

Kunci Kosakata & Rubrik Penilaian

Rubrik Penilaian Pengajar: Berikan 1 poin untuk setiap pencocokan yang benar (total 8 poin) dan setiap istilah konteks yang benar (total 6 poin).

POS 4: KUNCI PENCOCOKAN KONSEP

F 1. SPEAR	G 2. SPOOFING	D 3. SPF	H 4. DKIM
C 5. DMARC	B 6. WHALING	E 7. PHISHING	A 8. VISHING

POS 3: KUNCI ISTILAH KUNCI

1 SPEAR	2 SPOOFING	3 SPF	4 DKIM
5 DMARC	6 WHALING		

ALTERNATIF POS 6: KUNCI PENCOCOKAN KOSAKATA

1 B – SPOOFING	2 A – SPEAR	3 H – VISHING	4 C – SPF
5 G – PHISHING	6 E – DMARC	7 D – DKIM	8 F – WHALING

CATATAN DISKUSI UNTUK PENGAJAR

Istilah Kunci:
Pastikan siswa dapat menjelaskan SPEAR, SPOOFING, dan SPF dengan kata-kata sendiri serta memberi contoh untuk setiap istilah.

Studi Kasus:
Minta siswa mendukung rekomendasi mereka dengan fakta dari lembar kerja, bukan asumsi.

Evaluasi Sumber:
Minta siswa memeriksa setidaknya satu klaim terhadap referensi di lembar kerja, lalu diskusikan mengapa angka, harga, dan aturan dapat berubah seiring waktu.

Kunci Teka-Teki & Catatan Pengajar

JAWABAN PENCARIAN KATA

Y	P	X	F	P	L	C	S	R	I	G	N	R	M	P
X	Q	O	C	U	S	T	P	V	E	L	J	B	A	B
C	P	M	X	L	K	Y	E	K	I	X	T	K	D	Q
M	J	I	D	I	N	N	A	K	Q	S	P	G	M	M
Q	R	K	S	T	S	T	R	G	C	D	H	S	Q	O
G	H	D	S	B	P	W	P	D	S	Z	M	I	V	C
N	Z	W	F	K	O	H	Z	H	D	N	D	A	N	Q
I	X	P	C	U	O	B	A	Z	I	N	D	K	R	G
L	A	D	O	D	F	F	H	I	D	S	R	Q	M	C
A	E	I	R	Z	I	S	F	Q	V	F	H	A	A	Q
H	O	N	P	T	N	X	Q	K	R	U	S	I	D	N
W	Y	B	F	S	G	X	W	J	F	A	R	Z	N	Y
Y	L	G	I	M	R	J	M	P	L	T	O	H	Q	G
Q	H	Z	A	O	V	G	S	U	B	Y	R	Y	B	H
L	Z	G	J	O	P	N	W	C	M	Z	Y	G	Y	O

JAWABAN TEKA-TEKI SILANG



PANDUAN PENGAJAR UNTUK JAWABAN TEKA-TEKI SILANG

PETUNJUK MENDATAR

2 mendatar: DKIM Standar yang menambahkan tanda tangan kriptografis ke email (4 huruf)

3 mendatar: SPEAR ... phishing: email terarah untuk orang tertentu (5 huruf)

5 mendatar: SPOOFING Pemalsuan pengirim agar email tampak asli (8 huruf)

7 mendatar: WHALING Phishing yang mengincar eksekutif puncak (7 huruf)

PETUNJUK MENURUN

1 menurun: DMARC Aturan yang memberi tahu server cara menangani email yang gagal SPF atau DKIM (5 huruf)

4 menurun: PHISHING Pesan penipuan yang memancing pengguna membagikan data (8 huruf)

5 menurun: SPF Catatan DNS berisi daftar server email resmi (3 huruf)

6 menurun: VISHING Penipuan lewat panggilan telepon (7 huruf)

Kunci Jawaban Kata Acak & Sandi

Kunci penilaian untuk aktivitas menyusun kata acak dan Tantangan Sandi Rahasia.

KUNCI KATA ACAK

1. AESRP	SPEAR	5. FIPGOSNO	SPOOFING
2. FPS	SPF	6. IMDK	DKIM
3. ADCRM	DMARC	7. WNIGHLA	WHALING
4. SNGIHPHI	PHISHING	8. IHGVNIS	VISHING

KUNCI TANTANGAN SANDI RAHASIA

"PERIKSA PENGIRIM SEBELUM MENGKLIK"

Kunci Jawaban Studi Kasus

A Studi Kasus 1: Menangani Serangan Whaling pada Eksekutif

Jawaban Pengajar

PEDOMAN PENILAIAN

Jawaban siswa harus mencakup poin-poin berikut:

- Analisis Skenario: Seorang direktur keuangan menerima email yang sangat personal dan mengaku dari CEO, meminta transfer cepat $50.000 untuk menuntaskan pembelian domain rahasia.
- Strategi & Solusi yang Disarankan: Atur DMARC dengan kebijakan 'p=reject' untuk memblokir domain pengirim tiruan. Tambahkan spanduk peringatan pengirim eksternal di gerbang, dan wajibkan konfirmasi lisan di luar kanal untuk semua transaksi keuangan.

B Studi Kasus 2: Menerapkan Kebijakan Gerbang SPF/DKIM/DMARC

Jawaban Pengajar

PEDOMAN PENILAIAN

Jawaban siswa harus mencakup poin-poin berikut:

- Analisis Skenario: Sebuah perusahaan gagal audit keamanan karena email pemasarannya sering ditandai spam, dan peretas aktif memalsukan domain merek perusahaan.
- Strategi & Solusi yang Disarankan: Terbitkan catatan TXT SPF berisi IP pengirim resmi. Atur kunci tanda tangan DKIM di server email keluar, dan analisis laporan umpan balik XML DMARC untuk menemukan penyalahgunaan.