Nama: _____ Tanggal: _____ Nilai: _____

Penipuan Online & Rekayasa Sosial Perlindungan Endpoint

Phishing email, domain tiruan, vishing, penipuan dukungan teknis, verifikasi out-of-band, BEC

GAMBARAN PEMBELAJARAN PENIPUAN ONLINE

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 pertahanan dari penipuan online. Anda akan mempelajari situs phishing palsu, taktik rekayasa sosial, penipuan dukungan teknis, modus penipuan transfer, dan cara verifikasi pembayaran.

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/online-scams/

Peta Belajar Perlindungan dari Penipuan Online Anda

- Kenali tanda umum penipuan dukungan teknis dan domain typosquatting.
- Terapkan protokol verifikasi email (SPF, DKIM, DMARC) untuk melawan pemalsuan.
- Terapkan verifikasi transaksi di luar kanal untuk mencegah penipuan transfer bisnis.

PETUNJUK PANDUAN PENIPUAN ONLINE

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 perlindungan dari penipuan online. Akhiri dengan aktivitas bonus Berpikir Cepat.

PERLINDUNGAN DARI PENIPUAN ONLINE & REKAYASA SOSIAL (PENGANTAR)

Penipuan daring mengeksploitasi perilaku manusia melalui phishing, pop-up dukungan palsu, vishing, dan penipuan transfer dana. Menerapkan verifikasi transaksi out-of-band serta aturan domain SPF/DKIM/DMARC membantu memblokir vektor rekayasa sosial di gerbang.

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

Pos 1: Tantangan Pilihan Ganda

1. Apa tanda utama penipuan dukungan teknis?

- A. Pop-up yang mengaku sistem Anda terinfeksi dan meminta Anda menelepon suatu nomor
- B. Pembaruan keamanan otomatis dari registri resmi
- C. Pengelola kata sandi yang menolak mengisi kredensial di domain perusahaan
- D. Pencadangan berkas di latar belakang ke drive eksternal

2. Teknik mana yang memakai domain pengirim tiruan untuk mencuri data bank?

- A. Phishing email
- B. Pemindaian port
- C. Injeksi memori
- D. Penghancuran kriptografis

3. Apa yang dimaksud penipuan transfer?

- A. Menipu korban agar mengirim uang ke rekening perusahaan palsu lewat rekayasa sosial
- B. Mengenkripsi basis data sistem dengan ransomware
- C. Mengakses basis data lewat injeksi SQL
- D. Mencadangkan berkas sistem ke disk offline

4. Mengapa penipu membuat situs belanja palsu?

- A. Untuk mencuri data kartu kredit dan pembayaran pembeli
- B. Untuk menampung tabel analisis malware di sandbox
- C. Untuk mempercepat pengiriman pesanan online
- D. Untuk menguji desain situs web baru secara gratis

5. Apa arti vishing?

- A. Phishing suara lewat telepon untuk mencuri kredensial
- B. Memindai jaringan lokal untuk perangkat yang tidak aman
- C. Memulihkan basis data setelah pembobolan
- D. Menjalankan kode tak tepercaya di kontainer virtual

Pos 2: Tantangan Benar atau Salah

6 Pertanyaan 6

6. Penipuan phishing hanya mengincar pengguna biasa, tidak pernah eksekutif.

○ Benar ○ Salah

7 Pertanyaan 7

7. Domain tiruan sering memakai salah ketik kecil (seperti amaz0n.com) untuk meniru merek tepercaya.

○ Benar ○ Salah

8 Pertanyaan 8

8. Penipuan dukungan teknis bisa diatasi dengan memberi akses jarak jauh kepada penelepon.

○ Benar ○ Salah

9 Pertanyaan 9

9. Rekayasa sosial memanfaatkan psikologi manusia seperti rasa takut dan tergesa-gesa untuk melewati aturan keamanan.

○ Benar ○ Salah

10 Pertanyaan 10

10. Permintaan transfer harus selalu diverifikasi lewat kanal komunikasi lain.

○ 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. Email penipuan yang menjebak pengguna disebut _____ .
2. Alamat web yang meniru merek tepercaya disebut alamat _____ .
3. Penipuan suara yang mengincar data bank disebut _____ .
4. Pop-up yang meminta uang untuk menghapus virus adalah modus dukungan teknis berupa _____ .
5. Permintaan pembayaran harus dipastikan lewat kanal lain berupa _____ .
6. Mengalihkan transaksi bisnis ke rekening pencuri adalah penipuan _____ .

BANK KATA KOSAKATA

PENIPUAN PHISHING SMISHING TIRUAN TRANSFER VERIFIKASI VISHING WHALING

Tulis jawaban Anda di sini:

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

Pos 4: Pencocokan Konsep Keamanan

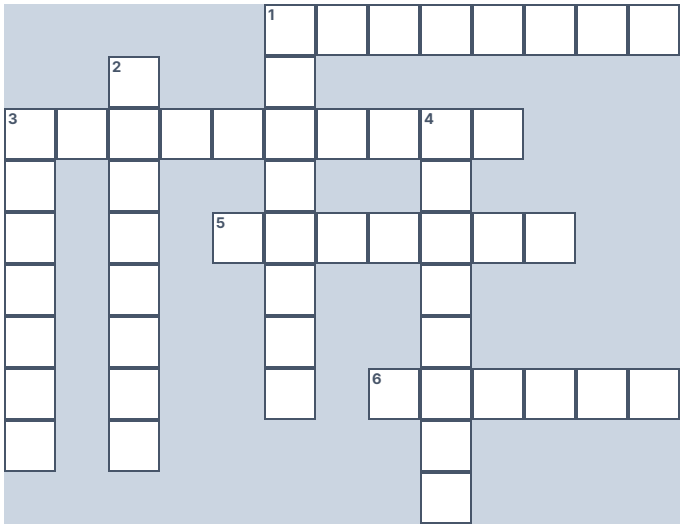
MENCOCOKKAN DEFINISI

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

☐	1. PHISHING	A	Pengalihan transaksi bank ke rekening penjahat.
☐	2. TIRUAN	B	Tipu daya untuk mencuri uang atau kredensial akses dari korban.
☐	3. VISHING	C	Mengirim SMS penipuan untuk mencuri kredensial akun seluler.
☐	4. PENIPUAN	D	Panggilan suara penipuan untuk mencuri kredensial dan data akun.
☐	5. VERIFIKASI	E	Serangan phishing terarah untuk mencuri kredensial eksekutif puncak.
☐	6. TRANSFER	F	Pengirim email atau alamat situs tiruan yang dibuat tampak asli.
☐	7. WHALING	G	Kampanye email penipuan untuk mencuri kredensial login dan kata sandi.
☐	8. SMISHING	H	Memastikan detail pembayaran lewat kontak kedua yang tepercaya.

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

1. Tipu daya, misalnya pop-up dukungan teknis palsu (8)

3. Konfirmasi pembayaran lewat kanal lain yang tepercaya (10)

5. Phishing terarah yang mengincar eksekutif puncak (7)

6. Jenis alamat web yang meniru merek terkenal (6)

PETUNJUK MENURUN

1. Email penipuan yang memancing pengguna menyerahkan login (8)

2. Pembayaran bank yang dialihkan penipu ke rekening mereka (8)

3. Penipuan lewat telepon untuk memancing data bank (7)

4. Penipuan lewat SMS berisi tautan ke portal palsu (8)

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

1 mendatar: Tipu daya, misalnya pop-up dukungan teknis palsu (8 huruf):

3 mendatar: Konfirmasi pembayaran lewat kanal lain yang tepercaya (10 huruf):

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

6 mendatar: Jenis alamat web yang meniru merek terkenal (6 huruf):

PETUNJUK MENURUN

1 menurun: Email penipuan yang memancing pengguna menyerahkan login (8 huruf):

2 menurun: Pembayaran bank yang dialihkan penipu ke rekening mereka (8 huruf):

3 menurun: Penipuan lewat telepon untuk memancing data bank (7 huruf):

4 menurun: Penipuan lewat SMS berisi tautan ke portal palsu (8 huruf):

Pos 6: Mencari Kata Tersembunyi

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

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

DAFTAR KOSAKATA

PHISHING TIRUAN VISHING PENIPUAN VERIFIKASI TRANSFER WHALING SMISHING

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. PHISHING
B. TIRUAN
C. VISHING
D. PENIPUAN
E. VERIFIKASI
F. TRANSFER
G. WHALING
H. SMISHING

DEFINISI & KOLOM PENCOCOKAN

1. Jenis alamat web yang meniru merek terkenal.
2. Konfirmasi pembayaran lewat kanal lain yang tepercaya.
3. Pembayaran bank yang dialihkan penipu ke rekening mereka.
4. Penipuan lewat SMS berisi tautan ke portal palsu.
5. Phishing terarah yang mengincar eksekutif puncak.
6. Penipuan lewat telepon untuk memancing data bank.
7. Email penipuan yang memancing pengguna menyerahkan login.
8. Tipu daya, misalnya pop-up dukungan teknis palsu.

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. **NSHPIHGI** _____
2. **VSGNIHI** _____
3. **VISKEFIIAR** _____
4. **GHILNWA** _____
5. **URNTAI** _____
6. **ANIUPPEN** _____
7. **TRSFERNA** _____
8. **SMHGSNII** _____

Aktivitas Bonus: Berpikir Cepat

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

1	Perangkat yang bisa diretas			
2	Kalimat yang sering dipakai penipu			
3	Metode pembayaran yang diminta penipu			
4	Jenis penipuan online			
5	Penawaran yang terlalu bagus untuk jadi nyata			
6	Tempat melaporkan penipuan			
7	Kata yang berkaitan dengan keamanan siber			
8	Orang yang bisa Anda peringatkan soal penipuan			
9	Hal yang Anda cadangkan			
10	Tanda bahaya dalam email			
11	Tanda komputer terinfeksi			
12	Cara memeriksa toko online			
13	Cara melindungi akun Anda			
14	Hal yang dilakukan jika tertipu			
15	Hal yang dilakukan setelah kebocoran data			

Pos 8: Studi Kasus Keamanan Siber

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

STUDI KASUS 1: MENCEGAH PENIPUAN TRANSFER PERUSAHAAN

👷

Skenario: Bagian keuangan menerima email mendesak dari alamat pemasok tiruan yang meminta pembayaran faktur berikutnya dikirim ke nomor rekening baru.

Pertanyaan Diskusi: Uraikan kebijakan verifikasi penipuan transfer, dan sebutkan pemblokiran lewat autentikasi email.

STUDI KASUS 2: INSIDEN PHISHING WHALING PADA EKSEKUTIF

👷

Skenario: Seorang eksekutif mengklik tautan phishing yang mengaku berisi dokumen rapat direksi, lalu memasukkan kredensial utama perusahaannya di portal tiruan.

Pertanyaan Diskusi: Uraikan langkah respons insiden, dan jelaskan cara mengaudit login eksekutif.

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

20	5	12	5	16	15	14		16	5	14	25	5	4	9	1		4	1	14

16	5	18	9	11	19	1

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 penipuan online?

Tipu daya lewat kanal digital untuk menjebak korban agar mengirim uang atau menyerahkan kredensial pribadi.

Q2: Apa tanda utama phishing email?

Pesan yang mendesak (seperti akun akan diblokir) dan mengarahkan ke tautan yang tidak cocok dengan domain resmi.

Q3: Apa itu typosquatting?

Mendaftarkan domain dengan salah ketik umum dari merek populer (seperti amaz0n.com) untuk situs phishing palsu.

Q4: Apa itu penipuan dukungan teknis?

Pop-up yang mengaku PC Anda terinfeksi dan menyuruh Anda menelepon lalu membayar perangkat lunak pembersih palsu atau layanan akses jarak jauh. [1]

Q5: Apa itu vishing?

Serangan phishing lewat panggilan telepon untuk menipu korban agar memberi data rekening atau login.

Pos 10: FAQ Dasar Keamanan Siber (Bagian B)

Pelajari pertanyaan dan jawaban umum tentang cara mengurangi ancaman online.

Q6: Apa arti penipuan transfer?

Pengalihan pembayaran ke rekening penipu dengan menyamar sebagai pemasok atau eksekutif.

Q7: Apa itu whaling?

Bentuk spear phishing yang sangat terarah pada sasaran bernilai tinggi seperti eksekutif puncak perusahaan.

Q8: Apa itu smishing?

SMS penipuan ke perangkat seluler berisi tautan ke portal palsu atau kabar pengiriman palsu.

Q9: Mengapa verifikasi di luar kanal sangat penting?

Detail transaksi dipastikan lewat kanal lain (seperti telepon), sehingga tidak bergantung pada email yang mungkin dibobol.

Q10: Bagaimana penipuan escrow palsu bekerja?

Penipu membuat situs escrow tiruan, mengaku dana disimpan aman, lalu mencuri setoran transfer pembeli.

Pos 10: FAQ Lanjutan Keamanan (Bagian C)

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

Q1: Bagaimana penipu memakai BEC (Business Email Compromise) untuk melakukan penipuan transfer dana?

Penipu membajak akun email karyawan asli, memantau percakapan faktur, lalu mengirim detail tagihan baru dengan rekening palsu.

Q2: Apa risiko serangan homograf IDN dalam penipuan online?

Memakai karakter non-ASCII yang tampak sama dengan huruf biasa (mis. 'a' Sirilik) untuk mendaftarkan domain tiruan yang meniru merek asli.

Q3: Mengapa pemeriksaan header email penting untuk mendeteksi penipuan?

Header menunjukkan IP server asal dan status validasi SPF/DKIM, sehingga terlihat apakah domain pengirim dipalsukan.

Q4: Bagaimana penipu dukungan teknis memanfaatkan perangkat lunak desktop jarak jauh?

Mereka memakai AnyDesk atau TeamViewer untuk masuk ke perangkat korban, menanam malware, dan mencuri kata sandi tersimpan.

Q5: Apa tujuan penipuan biaya di muka?

Menipu korban agar membayar biaya proses di muka demi imbalan besar yang sebenarnya tidak ada.

Pos 10: FAQ Lanjutan Keamanan (Bagian D)

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

Q6: Bagaimana penipu memakai profil media sosial untuk phishing terarah?

Mereka mengumpulkan struktur organisasi dan nama karyawan untuk menyusun email spear phishing yang meyakinkan.

Q7: Mengapa toko web palsu memberi diskon besar?

Untuk memancing pembeli memasukkan data kartu kredit, lalu memakainya ulang atau menjualnya di forum carding.

Q8: Bagaimana catatan DMARC memblokir penipuan phishing?

DMARC memungkinkan pemilik domain meminta penerima mengarantina atau menolak email yang gagal pemeriksaan SPF dan DKIM yang selaras, sehingga memblokir spoofing langsung. [5]

Q9: Apa ancaman portal pencuri kredensial?

Halaman tiruan yang dibuat persis seperti Microsoft 365 atau Google Workspace dan mencuri kredensial saat dimasukkan.

Q10: Bagaimana tim keamanan melaporkan dan menonaktifkan domain penipuan?

Dengan mengirim bukti penipuan ke email pengaduan registrar, penyedia hosting, dan registri Google Safe Browsing.

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. [2]

2. WAWASAN KEAMANAN

Business Email Compromise (BEC) menyebabkan kerugian lebih dari $3 miliar yang dilaporkan ke IC3 milik FBI pada 2025. [2]

3. WAWASAN KEAMANAN

Domain typo-squatting berbeda satu atau dua karakter dari nama merek asli, sehingga bisa terlewat jika hanya dilihat sekilas.

4. WAWASAN KEAMANAN

Penipuan dukungan teknis menyebabkan kerugian lebih dari $2.1 miliar yang dilaporkan ke IC3 milik FBI pada 2025. [2]

5. WAWASAN KEAMANAN

Serangan homograf tampak sama di bilah alamat browser kecuali browser menampilkan punycode.

6. WAWASAN KEAMANAN

Penipuan SMS (smishing) menggunakan pesan singkat yang mendesak disertai tautan, sehingga korban hanya punya sedikit konteks untuk mengenali penipuan.

7. WAWASAN KEAMANAN

Serangan whaling mengincar email eksekutif karena mereka mengendalikan transfer pembayaran besar.

8. WAWASAN KEAMANAN

Memverifikasi perubahan pembayaran dengan menelepon nomor telepon yang sudah dikenal dan tersimpan adalah pertahanan utama terhadap penipuan transfer BEC.

9. WAWASAN KEAMANAN

Situs escrow palsu adalah penipuan umum di marketplace online: tampak seperti layanan pembayaran aman, tetapi mencuri transfer bank pembeli.

10. WAWASAN KEAMANAN

Google Safe Browsing memperingatkan pengguna sebelum mereka membuka situs yang telah ditandainya sebagai phishing atau malware.

Referensi & Sumber Teknis

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

REFERENSI AKADEMIK & INDUSTRI

[1] Federal Trade Commission. (n.d.). How To Spot, Avoid, and Report Tech Support Scams.

https://consumer.ftc.gov/articles/how-spot-avoid-and-report-tech-support-scams

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

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

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

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

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

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

Kunci Jawaban: Pos 1 - Pilihan Ganda

1 Soal 1

Jawaban Benar: A

CATATAN PENGAJAR

Apa tanda utama penipuan dukungan teknis? → Pop-up yang mengaku sistem Anda terinfeksi dan meminta Anda menelepon suatu nomor

2 Soal 2

Jawaban Benar: A

CATATAN PENGAJAR

Teknik mana yang memakai domain pengirim tiruan untuk mencuri data bank? → Phishing email

3 Soal 3

Jawaban Benar: A

CATATAN PENGAJAR

Apa yang dimaksud penipuan transfer? → Menipu korban agar mengirim uang ke rekening perusahaan palsu lewat rekayasa sosial

4 Soal 4

Jawaban Benar: A

CATATAN PENGAJAR

Mengapa penipu membuat situs belanja palsu? → Untuk mencuri data kartu kredit dan pembayaran pembeli

5 Soal 5

Jawaban Benar: A

CATATAN PENGAJAR

Apa arti vishing? → Phishing suara lewat telepon untuk mencuri kredensial

Kunci Jawaban: Pos 2 - Benar atau Salah

6 **Soal 6** — **Jawaban Benar: Salah**

CATATAN PENGAJAR

Salah: phishing juga menyasar eksekutif; whaling adalah phishing yang ditujukan kepada pimpinan senior.

7 **Soal 7** — **Jawaban Benar: Benar**

CATATAN PENGAJAR

Domain tiruan sering memakai salah ketik kecil (seperti amaz0n.com) untuk meniru merek tepercaya.

8 **Soal 8** — **Jawaban Benar: Salah**

CATATAN PENGAJAR

Salah: memberi akses jarak jauh kepada penipu dukungan teknis memungkinkan mereka menanam malware dan mencuri data.

9 **Soal 9** — **Jawaban Benar: Benar**

CATATAN PENGAJAR

Rekayasa sosial memanfaatkan psikologi manusia seperti rasa takut dan tergesa-gesa untuk melewati aturan keamanan.

10 **Soal 10** — **Jawaban Benar: Benar**

CATATAN PENGAJAR

Permintaan transfer harus selalu diverifikasi lewat kanal komunikasi lain.

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

G 1. PHISHING	F 2. TIRUAN	D 3. VISHING	B 4. PENIPUAN
H 5. VERIFIKASI	A 6. TRANSFER	E 7. WHALING	C 8. SMISHING

POS 3: KUNCI ISTILAH KUNCI

1 PHISHING	2 TIRUAN	3 VISHING	4 PENIPUAN
5 VERIFIKASI	6 TRANSFER		

ALTERNATIF POS 6: KUNCI PENCOCOKAN KOSAKATA

1 B – TIRUAN	2 E – VERIFIKASI	3 F – TRANSFER	4 H – SMISHING
5 G – WHALING	6 C – VISHING	7 A – PHISHING	8 D – PENIPUAN

CATATAN DISKUSI UNTUK PENGAJAR

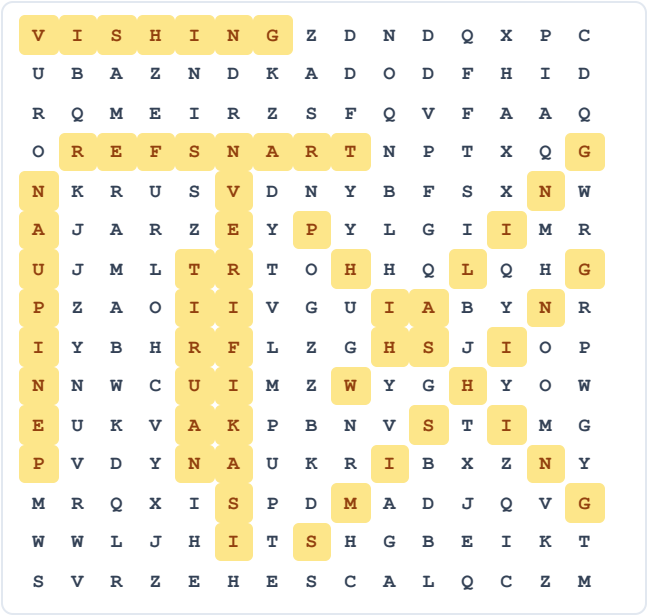
Istilah Kunci:
Pastikan siswa dapat menjelaskan PHISHING, TIRUAN, dan VISHING dengan kata-kata sendiri serta memberi contoh untuk setiap istilah.

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

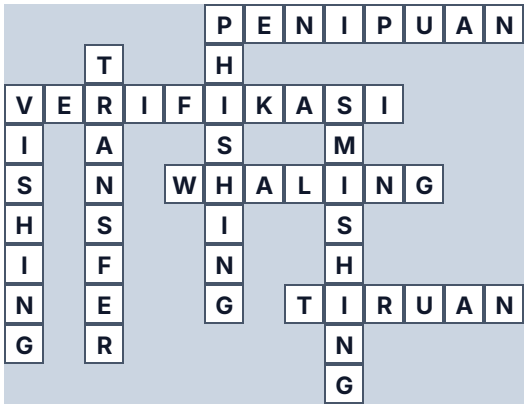
Evaluasi Sumber:
Minta siswa memeriksa setidaknya satu klaim terhadap referensi di lembar kerja, lalu diskusikan mengapa angka, harga, dan aturan dapat berubah seiring waktu.

Kunci Teka-Teki & Catatan Pengajar

JAWABAN PENCARIAN KATA



JAWABAN TEKA-TEKI SILANG



PANDUAN PENGAJAR UNTUK JAWABAN TEKA-TEKI SILANG

PETUNJUK MENDATAR

1 mendatar: PENIPUAN Tipu daya, misalnya pop-up dukungan teknis palsu (8 huruf)

3 mendatar: VERIFIKASI Konfirmasi pembayaran lewat kanal lain yang tepercaya (10 huruf)

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

6 mendatar: TIRUAN Jenis alamat web yang meniru merek terkenal (6 huruf)

PETUNJUK MENURUN

1 menurun: PHISHING Email penipuan yang memancing pengguna menyerahkan login (8 huruf)

2 menurun: TRANSFER Pembayaran bank yang dialihkan penipu ke rekening mereka (8 huruf)

3 menurun: VISHING Penipuan lewat telepon untuk memancing data bank (7 huruf)

4 menurun: SMISHING Penipuan lewat SMS berisi tautan ke portal palsu (8 huruf)

Kunci Jawaban Kata Acak & Sandi

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

KUNCI KATA ACAK

1. NSHPIHGI	PHISHING	5. URNTAI	TIRUAN
2. VSGNIHI	VISHING	6. ANIUPPEN	PENIPUAN
3. VISKEFIIAR	VERIFIKASI	7. TRSFERNA	TRANSFER
4. GHILNWA	WHALING	8. SMHGSNII	SMISHING

KUNCI TANTANGAN SANDI RAHASIA

"TELEPON PENYEDIA DAN PERIKSA"

Kunci Jawaban Studi Kasus

A Studi Kasus 1: Mencegah Penipuan Transfer Perusahaan

Jawaban Pengajar

PEDOMAN PENILAIAN

Jawaban siswa harus mencakup poin-poin berikut:

- Analisis Skenario: Bagian keuangan menerima email mendesak dari alamat pemasok tiruan yang meminta pembayaran faktur berikutnya dikirim ke nomor rekening baru.
- Strategi & Solusi yang Disarankan: Wajibkan otorisasi ganda untuk semua pembayaran. Terapkan verifikasi di luar kanal lewat nomor telepon yang sudah disimpan, dan blokir email domain tiruan di gerbang.

B Studi Kasus 2: Insiden Phishing Whaling pada Eksekutif

Jawaban Pengajar

PEDOMAN PENILAIAN

Jawaban siswa harus mencakup poin-poin berikut:

- Analisis Skenario: Seorang eksekutif mengklik tautan phishing yang mengaku berisi dokumen rapat direksi, lalu memasukkan kredensial utama perusahaannya di portal tiruan.
- Strategi & Solusi yang Disarankan: Isolasi perangkat eksekutif. Atur ulang semua token sesi dan kredensial perusahaan. Periksa log akses untuk data yang keluar, dan terapkan MFA perangkat keras di semua login.