Nama: _____ Tanggal: _____ Nilai: _____

Pencegahan Pencurian Identitas & Penyimpanan Perusahaan

Kebocoran kredensial, MFA, pemantauan dark web, peringatan pembekuan kredit, rekayasa sosial

GAMBARAN PEMBELAJARAN PENCEGAHAN PENCURIAN IDENTITAS

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 pencegahan dan mitigasi pencurian identitas. Anda akan mempelajari kebocoran kredensial, autentikasi multifaktor, pemantauan dark web, peringatan pembekuan kredit, dan pertahanan terhadap rekayasa sosial.

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/identity-theft/

Peta Belajar Perlindungan Identitas Anda

- Pahami risiko terbukanya kredensial di forum dark web.
- Terapkan autentikasi multifaktor (MFA) dan peringatan pembekuan kredit.
- Rancang pertahanan keamanan perusahaan terhadap penipuan rekayasa sosial yang terarah.

PETUNJUK PANDUAN PENCURIAN IDENTITAS

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 identitas. Akhiri dengan aktivitas bonus Berpikir Cepat.

PENCEGAHAN PENCURIAN IDENTITAS & KEAMANAN ASET (PENGANTAR)

Pencurian identitas memanfaatkan kredensial yang bocor dan login yang lemah untuk membajak akun pribadi maupun perusahaan. Menerapkan MFA, pembekuan kredit, pemindai dark web, dan kerangka SPF/DKIM/DMARC menjadi pertahanan penting terhadap peniruan identitas digital.

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

Pos 1: Tantangan Pilihan Ganda

1. Apa cara utama pencuri identitas mencuri kredensial login?

- A. Mengirim peringatan email palsu agar pengguna memasukkan kata sandi di portal tiruan
- B. Mendengarkan siaran radio di dekat kantor pengguna
- C. Mendefragmentasi penyimpanan server lokal pengguna
- D. Memutus konfigurasi cadangan jaringan eksternal

2. Kontrol keamanan mana yang paling kuat melawan kebocoran kredensial?

- A. Autentikasi multifaktor dengan kunci perangkat keras
- B. Membuat kata sandi panjang dengan format bawaan browser
- C. Mengganti nama pengguna email setiap enam bulan
- D. Menghapus cookie dan riwayat pelacakan browser

3. Apa yang dimaksud pembekuan kredit?

- A. Mengunci laporan kredit agar pencuri tidak bisa membuka pinjaman tanpa izin
- B. Menghapus riwayat transaksi rekening bank dari basis data
- C. Mematikan pembaca strip magnetik kartu kredit
- D. Mengenkripsi hard drive basis data lokal

4. Mengapa pemantauan dark web berguna?

- A. Memberi tahu pengguna jika kredensial mereka muncul di basis data ilegal
- B. Mencegah malware aktif berjalan di sandbox virtual
- C. Mempercepat perutean browser di jaringan virtual
- D. Memblokir upaya injeksi SQL ke basis data

5. Apa arti rekayasa sosial?

- A. Memanipulasi orang agar sukarela membuka kredensial rahasia
- B. Memindai port server perusahaan untuk celah keamanan
- C. Mencadangkan berkas basis data ke hard drive offline
- D. Merutekan paket lewat tiga node onion terenkripsi

Pos 2: Tantangan Benar atau Salah

6 Pertanyaan 6

6. Pencurian identitas hanya menyerang akun digital, bukan surat pos fisik.

○ Benar ○ Salah

7 Pertanyaan 7

7. Menerapkan MFA di semua akun pribadi memblokir sebagian besar serangan bot credential stuffing.

○ Benar ○ Salah

8 Pertanyaan 8

8. Pembekuan kredit memblokir pemeriksaan kredit tetapi juga membuat Anda tak bisa mengakses rekening sendiri.

○ Benar ○ Salah

9 Pertanyaan 9

9. Pengelola kata sandi melindungi dari phishing dengan menolak mengisi otomatis kata sandi di domain tiruan.

○ Benar ○ Salah

10 Pertanyaan 10

10. Email phishing sering memakai bahasa mendesak untuk memancing respons emosional yang cepat.

○ 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. Pencuri identitas mengincar kata sandi pribadi dan _____ .
2. Memberi tahu pengguna soal pembobolan basis data mengungkap akun pribadi yang mengalami _____ .
3. Kewajiban memasukkan kode sementara saat login disebut _____ .
4. Menelusuri forum peretas dark web untuk data curian disebut _____ .
5. Pemeriksaan kredit tanpa izin diblokir dengan _____ .
6. Melatih karyawan mengenali phishing membangun keamanan aktif berupa _____ .

BANK KATA KOSAKATA

KEBOCORAN KREDENSIAL MFA PEMANTAUAN PEMBEKUAN PERTAHANAN PHISHING SPOOFING

Tulis jawaban Anda di sini:

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

Pos 4: Pencocokan Konsep Keamanan

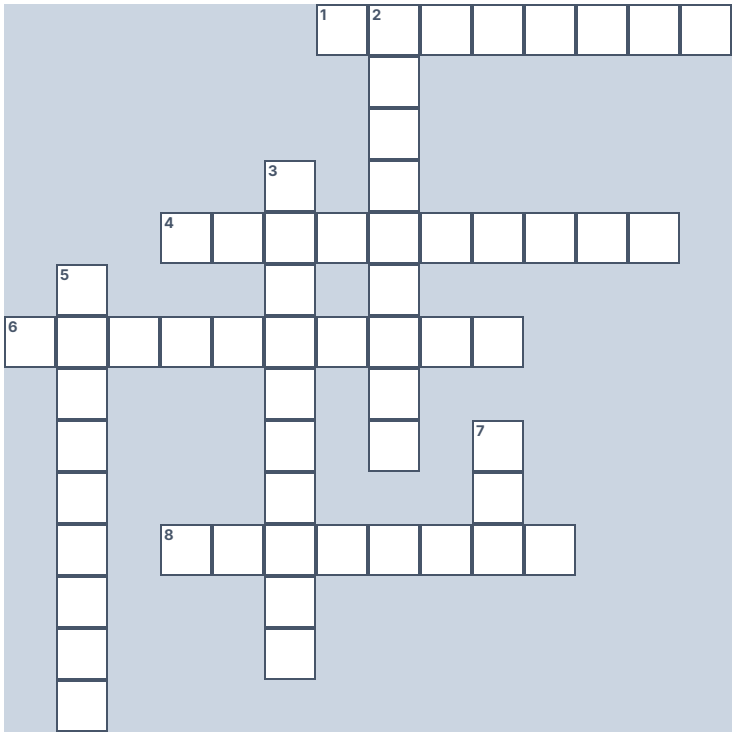
MENCOCOKKAN DEFINISI

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

☐	1. KREDENSIAL	A	Langkah verifikasi kedua (seperti kunci perangkat keras) yang melindungi login akun.
☐	2. KEBOCORAN	B	Membuat situs atau email palsu yang meniru organisasi asli.
☐	3. MFA	C	Membatasi akses ke berkas kredit untuk mencegah pengajuan pinjaman palsu.
☐	4. PEMANTAUAN	D	Terbukanya basis data pribadi berisi catatan pengguna tanpa izin.
☐	5. PEMBEKUAN	E	Pelatihan dan kontrol teknis untuk melindungi dari pencurian identitas.
☐	6. PERTAHANAN	F	Mengirim pesan penipuan agar pengguna menyerahkan kredensial.
☐	7. SPOOFING	G	Menelusuri forum online dan kanal peretas untuk data perusahaan yang dicuri.
☐	8. PENIPUAN	H	Nama pengguna, kata sandi, dan token pribadi untuk mengautentikasi identitas digital.

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. Situs atau email palsu yang meniru pengirim asli (8)

4. Nama pengguna dan kata sandi yang diincar pencuri identitas (10)

6. Penelusuran forum peretas untuk mencari data curian (10)

8. Pesan curang untuk memancing pengguna menyerahkan login (8)

PETUNJUK MENURUN

2. Pemblokiran pemeriksaan kredit agar tak ada pinjaman atas nama Anda (9)

3. Hal yang dibangun lewat pelatihan mengenali phishing (10)

5. Saat data pribadi keluar dari basis data tanpa izin (9)

7. Kewajiban kode atau kunci tambahan saat login (3)

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: Situs atau email palsu yang meniru pengirim asli (8 huruf):

4 mendatar: Nama pengguna dan kata sandi yang diincar pencuri identitas (10 huruf):

6 mendatar: Penelusuran forum peretas untuk mencari data curian (10 huruf):

8 mendatar: Pesan curang untuk memancing pengguna menyerahkan login (8 huruf):

PETUNJUK MENURUN

2 menurun: Pemblokiran pemeriksaan kredit agar tak ada pinjaman atas nama Anda (9 huruf):

3 menurun: Hal yang dibangun lewat pelatihan mengenali phishing (10 huruf):

5 menurun: Saat data pribadi keluar dari basis data tanpa izin (9 huruf):

7 menurun: Kewajiban kode atau kunci tambahan saat login (3 huruf):

Pos 6: Mencari Kata Tersembunyi

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

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

DAFTAR KOSAKATA

KREDENSIAL KEBOCORAN MFA PEMANTAUAN PEMBEKUAN PERTAHANAN SPOOFING PENIPUAN

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. KREDENSIAL
B. KEBOCORAN
C. MFA
D. PEMANTAUAN
E. PEMBEKUAN
F. PERTAHANAN
G. SPOOFING
H. PENIPUAN

DEFINISI & KOLOM PENCOCOKAN

1. Pesan curang untuk memancing pengguna menyerahkan login.
2. Nama pengguna dan kata sandi yang diincar pencuri identitas.
3. Situs atau email palsu yang meniru pengirim asli.
4. Hal yang dibangun lewat pelatihan mengenali phishing.
5. Penelusuran forum peretas untuk mencari data curian.
6. Pemblokiran pemeriksaan kredit agar tak ada pinjaman atas nama Anda.
7. Saat data pribadi keluar dari basis data tanpa izin.
8. Kewajiban kode atau kunci tambahan saat login.

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. **ASNERKILDE** _____
2. **AFM** _____
3. **PKEEUNBAM** _____
4. **ONGIFSPO** _____
5. **RCENOOKAB** _____
6. **ANAAUPETNM** _____
7. **ETPAHNANAR** _____
8. **IEPNPAUN** _____

Aktivitas Bonus: Berpikir Cepat

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

1	Hal yang dilakukan jika identitas dicuri			
2	Hal yang tidak boleh dibagikan di media sosial			
3	Hal yang Anda cadangkan			
4	Kartu atau identitas di dompet Anda			
5	Dokumen yang harus dijaga			
6	Hal yang dilakukan setelah kebocoran data			
7	Alasan memperbarui perangkat lunak			
8	Data yang diincar pencuri identitas			
9	Perangkat yang bisa diretas			
10	Tempat data Anda bisa bocor			
11	Kebiasaan aman yang bisa dimulai hari ini			
12	Tanda komputer terinfeksi			
13	Cara membuktikan identitas Anda			
14	Tanda pencurian identitas			
15	Tanda bahaya dalam email			

Pos 8: Studi Kasus Keamanan Siber

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

STUDI KASUS 1: PERLINDUNGAN DARI PENIRUAN IDENTITAS EKSEKUTIF



Skenario: Seorang eksekutif puncak ternama menjadi sasaran domain typo-squatting yang meniru email pribadinya untuk menipu klien. Rancang rencana perlindungan merek.

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

STUDI KASUS 2: KREDENSIAL PERUSAHAAN TERBUKA DI DARK WEB



Skenario: Sebuah bocoran basis data di dark web berisi ratusan kredensial perusahaan milik administrator sistem sebuah perusahaan. Rancang strategi mitigasi.

Pertanyaan Diskusi: Uraikan proses pembersihan kredensial, dan rencanakan peluncuran pengelola kata sandi.

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

12	9	14	4	21	14	7	9		9	4	5	14	20	9	20	1	19

1	14	4	1		4	5	14	7	1	14		13	6	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 pencurian identitas?

Kejahatan saat penyerang mencuri data pribadi (seperti kata sandi atau nomor jaminan sosial) untuk menyamar sebagai orang lain demi keuntungan finansial.

Q2: Apa penyebab paling umum pencurian identitas?

Phishing adalah cara utama pencuri mendapatkan kata sandi, dengan memancing pengguna ke situs web palsu yang meniru situs asli.

Q3: Bagaimana autentikasi multifaktor (MFA) melindungi identitas?

MFA meminta bukti kedua (seperti kunci perangkat keras) saat login, sehingga penyerang tetap terblokir meski mencuri kata sandi Anda.

Q4: Apa itu pembekuan kredit?

Layanan gratis yang mencegah biro kredit membagikan berkas kredit Anda, sehingga pencuri tak bisa membuka pinjaman atas nama Anda. [2]

Q5: Apa itu pemantauan dark web?

Perangkat lunak yang memeriksa forum peretas untuk email, kata sandi, dan data pribadi yang bocor, lalu memberi tahu Anda jika data Anda terbuka.

Pos 10: FAQ Dasar Keamanan Siber (Bagian B)

Pelajari pertanyaan dan jawaban umum tentang cara mengurangi ancaman online.

Q6: Apa arti credential stuffing?

Bot otomatis yang mencoba daftar kata sandi bocor di ratusan situs untuk mengambil alih akun aktif.

Q7: Mengapa email spoofing berbahaya?

Penyerang dapat memalsukan nama pengirim email, sehingga pesan phishing tampak berasal dari rekan tepercaya.

Q8: Bagaimana pengelola kata sandi mencegah pencurian identitas?

Pengelola kata sandi menyimpan kata sandi rumit dan unik untuk tiap akun serta menolak mengisi otomatis di domain phishing palsu.

Q9: Apa itu spear phishing?

Serangan phishing yang sangat terarah dengan nama dan detail korban agar peluang menipu lebih besar.

Q10: Apa beda peringatan kredit dengan pembekuan?

Peringatan meminta pemberi pinjaman memverifikasi identitas Anda sebelum membuka akun, sedangkan pembekuan memblokir akses ke berkas kredit sepenuhnya. [2]

Pos 10: FAQ Lanjutan Keamanan (Bagian C)

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

Q1: Bagaimana SIM swapping berujung pada pencurian identitas?

Penyerang membujuk staf operator memindahkan nomor telepon korban ke kartu SIM baru, lalu membajak kode 2FA lewat SMS.

Q2: Apa peran DMARC dalam mencegah pencurian identitas?

DMARC memungkinkan pemilik domain memblokir email tiruan agar tidak sampai ke kotak masuk, sehingga email palsu tak bisa meniru domain perusahaan.

Q3: Mengapa pencurian identitas sintetis sulit dideteksi?

Pencuri menggabungkan nomor jaminan sosial asli dengan nama dan tanggal lahir palsu untuk membuat profil kredit baru yang lolos dari peringatan penipuan dasar.

Q4: Bagaimana pialang data memanfaatkan identitas pribadi?

Pialang mengumpulkan catatan publik, perilaku web, dan riwayat pembelian menjadi berkas profil yang bisa bocor atau dijual.

Q5: Mengapa MFA berbasis SMS dianggap rentan?

Lalu lintas SMS rentan disadap, di-phishing, dan dieksploitasi lewat SIM swapping di tingkat operator.

Pos 10: FAQ Lanjutan Keamanan (Bagian D)

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

Q6: Apa itu penguncian berkas kredit?

Layanan komersial mirip pembekuan yang memungkinkan pengguna langsung mengunci atau membuka berkas kredit lewat aplikasi seluler.

Q7: Bagaimana pembobolan data perusahaan memicu pencurian identitas?

Basis data yang bocor membuka jutaan kredensial tanpa enkripsi, memberi pencuri bahan mentah untuk penipuan identitas yang terarah.

Q8: Apa risiko terlalu banyak berbagi di media sosial?

Membagikan nama hewan peliharaan, tempat lahir, dan nama gadis ibu memberi pencuri jawaban atas pertanyaan pemulihan akun yang umum.

Q9: Bagaimana login biometrik melindungi profil identitas?

Biometrik mengaitkan login dengan ciri seperti sidik jari atau wajah; jika disimpan di perangkat, data ini sulit dicuri, tetapi data biometrik yang tersimpan dapat bocor.

Q10: Bagaimana Red Flags Rule memerangi pencurian identitas?

Peraturan federal yang mewajibkan lembaga keuangan menyusun program tertulis untuk mendeteksi dan menanggapi tanda bahaya pencurian identitas.

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

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

1. WAWASAN KEAMANAN

IdentityTheft.gov, yang dikelola FTC, memungkinkan korban di AS melaporkan pencurian identitas dan mendapatkan rencana pemulihan pribadi. [1]

2. WAWASAN KEAMANAN

Kunci keamanan perangkat keras adalah MFA yang tahan phishing, jenis MFA terkuat yang didorong oleh CISA. [4]

3. WAWASAN KEAMANAN

Kata sandi yang disusupi adalah titik masuk umum dalam kebocoran data, yang kemudian memicu penipuan identitas.

4. WAWASAN KEAMANAN

Pembekuan kredit gratis menurut hukum federal dan mencegah pemberi pinjaman memeriksa berkas kredit sampai dibuka. [2]

5. WAWASAN KEAMANAN

DMARC memungkinkan pemilik domain meminta server email menolak atau mengarantina email palsu yang gagal pemeriksaan. [7]

6. WAWASAN KEAMANAN

SIM swapping memungkinkan peretas melewati autentikasi dua faktor berbasis SMS di portal perbankan.

7. WAWASAN KEAMANAN

Penipuan identitas sintetis mencampur data asli dan palsu, sehingga sulit dideteksi oleh pemberi pinjaman.

8. WAWASAN KEAMANAN

Banyak orang menggunakan ulang kata sandi yang sama di berbagai akun daring, sehingga satu kebocoran dapat membuka beberapa akun sekaligus.

9. WAWASAN KEAMANAN

Pialang data menyusun dosier terperinci tentang banyak sekali konsumen, sehingga menimbulkan risiko privasi yang terpusat.

10. WAWASAN KEAMANAN

Pemulihan dari pencurian identitas dapat memakan waktu berbulan-bulan, misalnya untuk menyanggah tagihan dan memperbaiki laporan kredit.

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.). IdentityTheft.gov: Report identity theft and get a recovery plan.
https://www.identitytheft.gov/

[2] Federal Trade Commission. (2025). Credit Freezes and Fraud Alerts.
https://consumer.ftc.gov/articles/credit-freezes-and-fraud-alerts

[3] Federal Trade Commission. (n.d.). What To Know About Identity Theft.
https://consumer.ftc.gov/articles/what-know-about-identity-theft

[4] CISA. (n.d.). More than a Password.
https://www.cisa.gov/MFA

[5] 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

[6] NIST. (2025). SP 800-63B-4: Digital Identity Guidelines: Authentication and Authenticator Management.
https://pages.nist.gov/800-63-4/sp800-63b.html

[7] 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 cara utama pencuri identitas mencuri kredensial login? → Mengirim peringatan email palsu agar pengguna memasukkan kata sandi di portal tiruan

2 Soal 2 — **Jawaban Benar: A**

CATATAN PENGAJAR

Kontrol keamanan mana yang paling kuat melawan kebocoran kredensial? → Autentikasi multifaktor dengan kunci perangkat keras

3 Soal 3 — **Jawaban Benar: A**

CATATAN PENGAJAR

Apa yang dimaksud pembekuan kredit? → Mengunci laporan kredit agar pencuri tidak bisa membuka pinjaman tanpa izin

4 Soal 4 — **Jawaban Benar: A**

CATATAN PENGAJAR

Mengapa pemantauan dark web berguna? → Memberi tahu pengguna jika kredensial mereka muncul di basis data ilegal

5 Soal 5 — **Jawaban Benar: A**

CATATAN PENGAJAR

Apa arti rekayasa sosial? → Memanipulasi orang agar sukarela membuka kredensial rahasia

Kunci Jawaban: Pos 2 - Benar atau Salah

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

CATATAN PENGAJAR

Pencurian identitas juga bisa berawal secara offline, misalnya dari surat atau dokumen yang dicuri.

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

CATATAN PENGAJAR

Menerapkan MFA di semua akun pribadi memblokir sebagian besar serangan bot credential stuffing.

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

CATATAN PENGAJAR

Pembekuan kredit menghentikan pemeriksaan kredit baru tetapi tidak memengaruhi akun Anda yang sudah ada.

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

CATATAN PENGAJAR

Pengelola kata sandi melindungi dari phishing dengan menolak mengisi otomatis kata sandi di domain tiruan.

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

CATATAN PENGAJAR

Email phishing sering memakai bahasa mendesak untuk memancing respons emosional yang cepat.

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

H 1. KREDENSIAL	D 2. KEBOCORAN	A 3. MFA	G 4. PEMANTAUAN
C 5. PEMBEKUAN	E 6. PERTAHANAN	B 7. SPOOFING	F 8. PENIPUAN

POS 3: KUNCI ISTILAH KUNCI

1 KREDENSIAL	2 KEBOCORAN	3 MFA	4 PEMANTAUAN
5 PEMBEKUAN	6 PERTAHANAN		

ALTERNATIF POS 6: KUNCI PENCOCOKAN KOSAKATA

1 H – PENIPUAN	2 A – KREDENSIAL	3 G – SPOOFING	4 F – PERTAHANAN
5 D – PEMANTAUAN	6 E – PEMBEKUAN	7 B – KEBOCORAN	8 C – MFA

CATATAN DISKUSI UNTUK PENGAJAR

Istilah Kunci:
Pastikan siswa dapat menjelaskan KREDENSIAL, KEBOCORAN, dan MFA dengan kata-kata sendiri serta memberi contoh untuk setiap istilah.

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

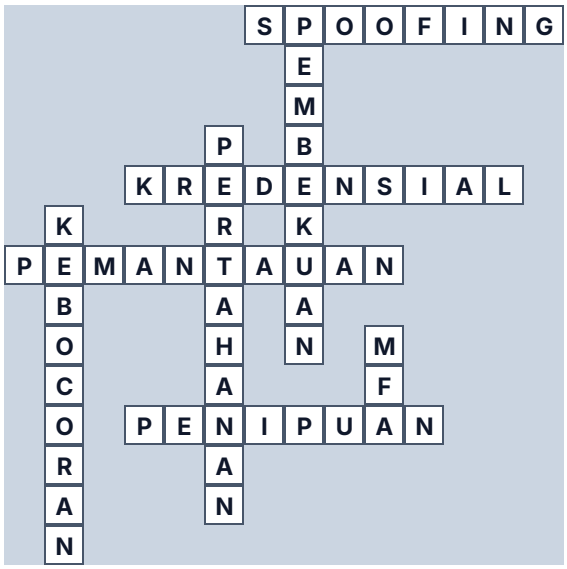
Evaluasi Sumber:
Minta siswa memeriksa setidaknya satu klaim terhadap referensi di lembar kerja, lalu diskusikan mengapa angka, harga, dan aturan dapat berubah seiring waktu.

Kunci Teka-Teki & Catatan Pengajar

JAWABAN PENCARIAN KATA

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

JAWABAN TEKA-TEKI SILANG



PANDUAN PENGAJAR UNTUK JAWABAN TEKA-TEKI SILANG

PETUNJUK MENDATAR

1 mendatar: SPOOFING Situs atau email palsu yang meniru pengirim asli (8 huruf)

4 mendatar: KREDENSIAL Nama pengguna dan kata sandi yang diincar pencuri identitas (10 huruf)

6 mendatar: PEMANTAUAN Penelusuran forum peretas untuk mencari data curian (10 huruf)

8 mendatar: PENIPUAN Pesan curang untuk memancing pengguna menyerahkan login (8 huruf)

PETUNJUK MENURUN

2 menurun: PEMBEKUAN Pemblokiran pemeriksaan kredit agar tak ada pinjaman atas nama Anda (9 huruf)

3 menurun: PERTAHANAN Hal yang dibangun lewat pelatihan mengenali phishing (10 huruf)

5 menurun: KEBOCORAN Saat data pribadi keluar dari basis data tanpa izin (9 huruf)

7 menurun: MFA Kewajiban kode atau kunci tambahan saat login (3 huruf)

Kunci Jawaban Kata Acak & Sandi

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

KUNCI KATA ACAK

1. A S N E R K I L D E — **KREDENSIAL**
2. A F M — **MFA**
3. P K E E U N B A M — **PEMBEKUAN**
4. O N G I F S P O — **SPOOFING**
5. R C E N O O K A B — **KEBOCORAN**
6. A N A A U P E T N M — **PEMANTAUAN**
7. E T P A H N A N A R — **PERTAHANAN**
8. I E P N P A U N — **PENIPUAN**

KUNCI TANTANGAN SANDI RAHASIA

"LINDUNGI IDENTITAS ANDA DENGAN MFA"

Kunci Jawaban Studi Kasus

A Studi Kasus 1: Perlindungan dari Peniruan Identitas Eksekutif

Jawaban Pengajar

PEDOMAN PENILAIAN

Jawaban siswa harus mencakup poin-poin berikut:

- Analisis Skenario: Seorang eksekutif puncak ternama menjadi sasaran domain typo-squatting yang meniru email pribadinya untuk menipu klien. Rancang rencana perlindungan merek.
- Strategi & Solusi yang Disarankan: Daftarkan semua variasi ejaan umum nama eksekutif. Terapkan protokol autentikasi email (DMARC, DKIM, SPF) untuk mencegah peniruan domain. Wajibkan MFA perangkat keras di semua login perusahaan para eksekutif puncak.

B Studi Kasus 2: Kredensial Perusahaan Terbuka di Dark Web

Jawaban Pengajar

PEDOMAN PENILAIAN

Jawaban siswa harus mencakup poin-poin berikut:

- Analisis Skenario: Sebuah bocoran basis data di dark web berisi ratusan kredensial perusahaan milik administrator sistem sebuah perusahaan. Rancang strategi mitigasi.
- Strategi & Solusi yang Disarankan: Lakukan pengaturan ulang kata sandi di seluruh perusahaan. Wajibkan pengelola kata sandi perusahaan. Terapkan MFA di semua portal sistem dan pasang peringatan pemantauan dark web otomatis yang berkelanjutan.