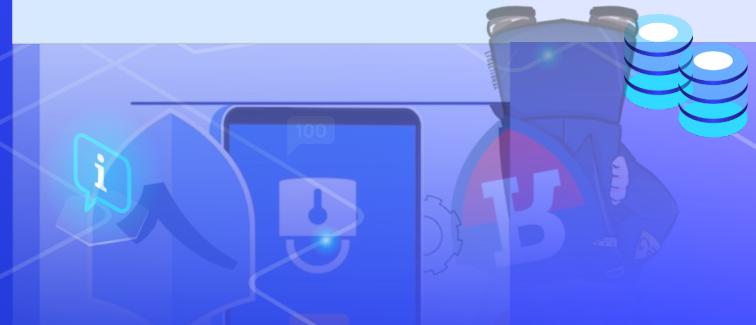




Aman Menggunakan Smartphone dari Serangan Siber

- by Restia Moegiono, S.ST. {CEH|CHFI|ECSA|QRMO}
- Sosialisasi Security Awareness Jakarta Barat
- Jum'at, 22 Maret 2024

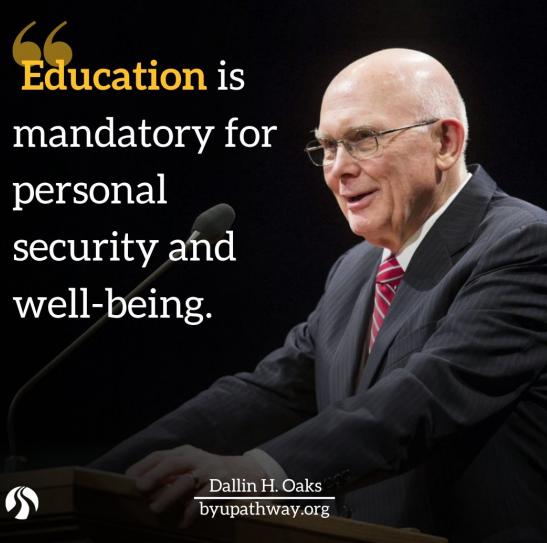


**“FUTURE IS MOBILE COMPUTING -
SMARTPHONES AND TABLETS ARE JUST
ELEMENTS OF IT. THE INDUSTRY IS ON THE
VERGE OF A WHOLE NEW PARADIGM.”**

THORSTEIN HEINS

© Lifehack Quotes

“**Education** is mandatory for personal security and well-being.



Dallin H. Oaks
byupathway.org



Kominfotik
Jakarta Barat

“
CYBERSECURITY IS A SHARED RESPONSIBILITY, AND IT BOILS DOWN TO THIS: IN CYBERSECURITY, THE MORE SYSTEMS WE SECURE, THE MORE SECURE WE ALL ARE.

- Jeh Johnson

“ Awareness of threats is the key to preventing cyber attacks.

Pentingnya Smartphone Security

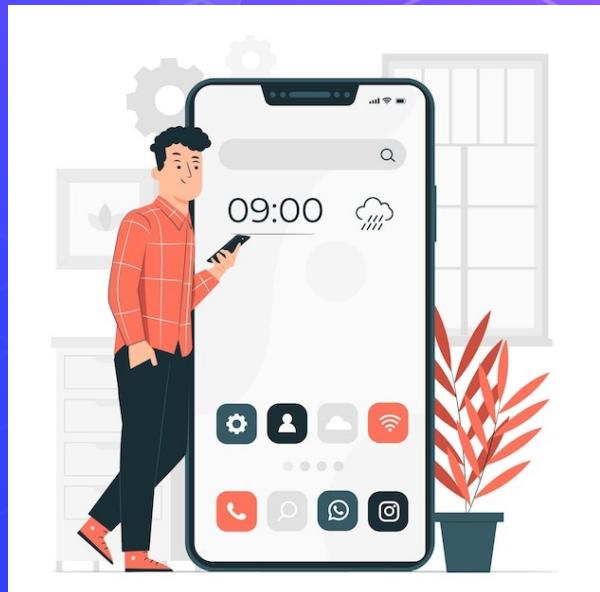


POWERED BY GOLDPHISH®



Overview

- Arti pentingnya *smartphone* untuk pengguna
- Aspek keamanan informasi pada *smartphone*
- 10 ancaman/risiko pada *smartphone*
- 6 serangan siber pada *smartphone*:
 - Aplikasi *spyware*
 - Aplikasi *diallerware*
 - Aplikasi *financial malware*
 - Aplikasi *mobile ransomware*
- Serangan *phishing*
 - Apa itu *social engineering*?
 - Bagaimana *social engineering* terjadi?
 - Tanda-tanda serangan *social engineering*
 - Cara mengatasi *phishing*
 - Bagaimana MFA dapat mengatasi *phishing*?
 - Penanganan *phishing* pada organisasi
- Ciri-ciri *smartphone* yang terkena serangan siber
- Cara mencegah serangan siber pada *smartphone*
- Penanganan serangan siber pada *smartphone*



Arti Pentingnya Smartphone untuk Pengguna

No.	Atribut Smartphone	Alasan
1.	Perangkat smartphone itu sendiri	<ul style="list-style-type: none">▪ Memuat informasi digital▪ Harga belinya relatif mahal
2.	SIM Card	SIM Card dibutuhkan untuk berkomunikasi dengan teknologi selular
3.	Foto	<ul style="list-style-type: none">▪ Foto memuat informasi digital yang berharga bagi pengguna▪ Kenangan bagi pengguna
4.	Daftar kontak	Informasi untuk bisa menghubungi orang lain yang berelasi
5.	Aplikasi pribadi, misalnya mobile banking, e-commerce, e-health	<ul style="list-style-type: none">▪ Aplikasi memuat informasi digital yang berharga bagi kehidupan pribadi▪ Aplikasi mempermudah kehidupan pribadi
6.	Email	Kemudahan mengakses melalui smartphone melalui aplikasi email client
7.	Aplikasi yang berhubungan dengan pekerjaan, misalnya cloud storage, absensi mobile, e-office	<ul style="list-style-type: none">▪ Aplikasi memuat informasi digital yang berharga bagi pekerjaan▪ Aplikasi di smartphone mempermudah pekerjaan
8.	Musik	Pengguna memiliki playlist yang disimpan di smartphone
9.	Dokumen	Dokumen memuat informasi digital yang berharga bagi pengguna
10.	Video	<ul style="list-style-type: none">▪ Video memuat informasi digital yang berharga bagi pengguna▪ Kenangan bagi pengguna
11.	Pesan teks, misalnya pesan chat dan SMS	<ul style="list-style-type: none">▪ Pesan teks memuat informasi digital yang berharga bagi pengguna▪ Kenangan bagi pengguna

Aspek Keamanan Informasi pada Smartphone

Smartphone merupakan perangkat pengguna yang mengelola informasi digital. Oleh karena itu, pengguna perlu memahami keamanan informasi digital pada smartphone pada 3 (tiga) aspek, yaitu:



Kerahasiaan

Informasi digital pada smartphone harus dilindungi kerahasiaannya agar informasi hanya dapat diakses oleh pengguna yang berhak dan dicegah dari akses pihak lain yang tidak berhak. Misalnya penerapan *end-to-end encryption*.



Integritas

Informasi digital pada smartphone harus dilindungi integritasnya agar tidak diubah oleh pihak lain yang tidak berhak. Misalnya penerapan *screen lock* dan *download* aplikasi dari Play Store/App Store.



Ketersediaan

Informasi digital pada smartphone harus dilindungi ketersediaannya agar dapat diakses setiap kali dibutuhkan. Misalnya melakukan *backup* secara berkala dan penggunaan *cloud storage*.

10 Ancaman/Risiko pada Smartphone

Pada smartphone, setidaknya terdapat 10 (sepuluh) ancaman/risiko yaitu:

No.	Risiko/Ancaman	Detail Risiko/Ancaman	Dampak
1.	Smartphone hilang/dicuri	Smartphone hilang/dicuri dan media penyimpanan di dalamnya tidak terlindungi, sehingga memungkinkan penjahat siber mengakses data yang tersimpan di dalamnya	<ul style="list-style-type: none">• Kebocoran data pribadi ke publik sehingga reputasi memburuk• Kerugian finansial• Operasional smartphone terhambat
2.	Penonaktifan smartphone yang tidak tepat	Smartphone dinonaktifkan (dijual/dibuang) secara tidak aman, sehingga informasi digital di dalamnya masih bisa diungkapkan	Kebocoran data pribadi ke publik sehingga reputasi memburuk
3.	Pengaturan privasi yang kurang sesuai	Pengguna smartphone tidak sengaja mengungkapkan informasi pada aplikasi karena pengaturan privasi yang kurang sesuai : <i>user permission</i> , keamanan aplikasi yang lemah, tidak melakukan <i>hardening</i> atau tidak melakukan <i>setting</i> privasi	Kebocoran data pribadi ke publik sehingga reputasi memburuk
4.	Serangan <i>phishing</i>	Penjahat siber mengumpulkan kredensial pengguna (seperti <i>password</i> dan nomor kartu ATM) menggunakan pesan yang mengelabui sehingga korban : melakukan instalasi <i>malware</i> atau mengungkapkan informasi kredensial secara sukarela	<ul style="list-style-type: none">• Kebocoran data pribadi ke publik sehingga reputasi memburuk• Kerugian finansial• Operasional smartphone terhambat

10 Ancaman/Risiko pada Smartphone

001

No.	Risiko/Ancaman	Detail Risiko/Ancaman	Dampak
5.	Aplikasi spyware	Smartphone memiliki spyware yang terinstal, sehingga memungkinkan penjahat siber memata-matai korban yang ditargetkan	Kebocoran data pribadi ke publik sehingga reputasi memburuk
6.	Pengawasan/memata-matai (surveillance)	Surveillance mencakup tindakan memata-matai korban yang tidak ditargetkan dengan mengumpulkan data pribadi	Kebocoran data pribadi ke pihak tertentu
7.	Serangan rogue hotspot	Penjahat siber meletakkan WiFi publik palsu (<i>rogue hotspot</i>) agar pengguna terhubung, kemudian akan menyadap/merusak komunikasi pengguna untuk mendapatkan kredensial	<ul style="list-style-type: none">• Kebocoran data pribadi ke publik sehingga reputasi memburuk• Kerugian finansial
8.	Serangan diallerware	Penjahat siber mencuri uang dari pengguna melalui <i>malware</i> yang membuat korban berlangganan layanan telepon premium atau SMS premium	Kerugian finansial
9.	Financial malware	Smartphone terinfeksi <i>malware</i> yang dirancang khusus untuk mencuri atau merusak transaksi kredensial <i>mobile banking</i>	Kerugian finansial
10.	Mobile ransomware	Smartphone terinfeksi <i>malware</i> yang dirancang khusus untuk mengenkripsi data atau membocorkan data, kemudian meminta tebusan untuk mendekripsi data atau mencegah data dibocorkan ke publik	<ul style="list-style-type: none">• Kebocoran data pribadi ke publik sehingga reputasi memburuk• Kerugian finansial• Operasional smartphone terhambat

6 Serangan Siber pada Smartphone



Aplikasi *spyware*



Aplikasi *diallerware*



Mobile *Ransomware*



Serangan *Phishing*



Serangan *Rogue Hotspot*



Aplikasi *financial malware*



Aplikasi Spyware

- Spyware itu aplikasi yang licik, dan sangat pandai menyembunyikan dirinya sendiri. Biasanya, ia melakukan ini dengan melampirkan dirinya ke sistem operasi dan berjalan di *background* sebagai program memori-residen.
- Spyware bahkan bisa datang dengan program yang tampak sah, dengan unduhan (*download*) yang cerdik atau melalui serangan *phishing*.
- Spyware pada smartphone dapat melakukan :
 1. Melacak lokasi geografis pengguna, log panggilan, daftar kontak, dan bahkan foto yang diambil di kamera smartphone.
 2. Merekam suara dan mengirimkan informasinya ke pihak ketiga, bahkan melakukan streaming langsung kamera pengguna ke internet, dan menjalankan perangkat lunak pengenalan wajah di wajah pengguna.

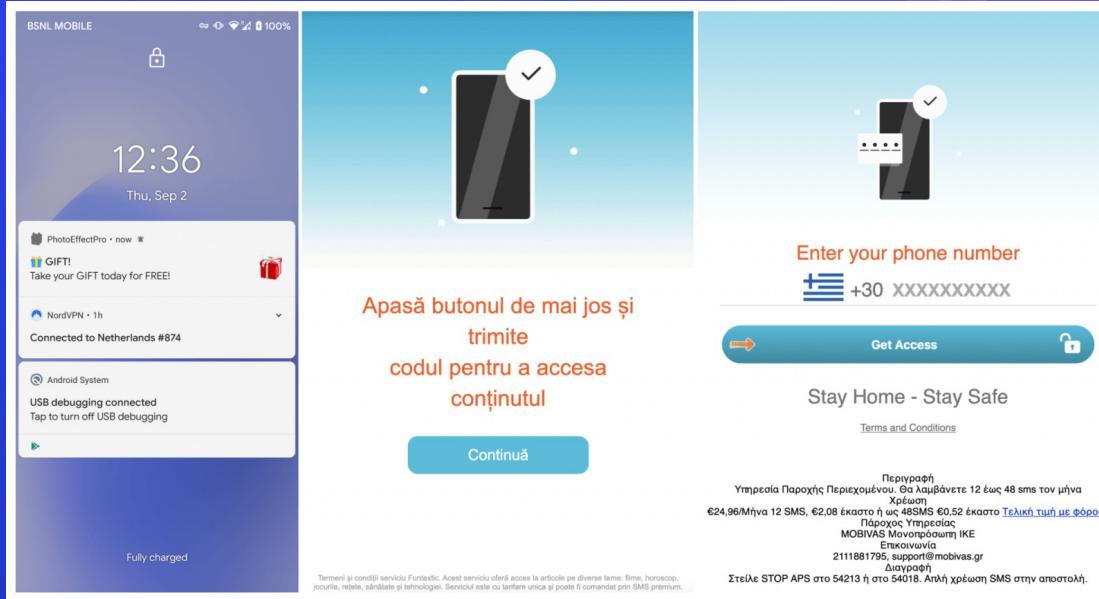
Aplikasi Spyware





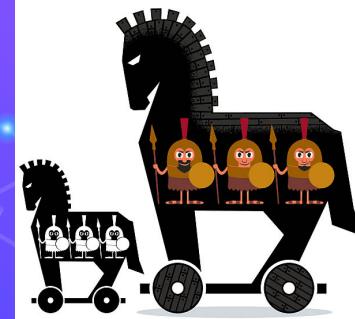
Aplikasi Diallerware

- API fitur panggilan pada smartphone tertentu terkadang membebani uang kepada pengguna, mis. SMS dan telepon premium.
- **Aplikasi diallerware** pada smartphone dapat melakukan panggilan API tersebut secara diam-diam atau mengelabui pengguna agar memberikan persetujuan, sehingga dapat mencuri uang dari pengguna smartphone.
- *Diallerware GriftHorse pada 2021 ditemukan oleh tim keamanan Zimperium.*



1. GriftHorse menyusup di dalam aplikasi yang tampaknya tidak berbahaya.
2. GriftHorse akan membombardir pengguna dengan peringatan (notifikasi pop-up yang muncul sekitar lima kali per jam) bahwa pengguna telah memenangkan hadiah dan harus segera mengklaimnya.
3. Setelah di-klik GriftHorse mengarahkan pengguna ke halaman web yang meminta nomor telepon untuk verifikasi.
4. Pengguna secara tidak sadar telah mendaftarkan diri ke layanan SMS premium dengan biaya langganan sebesar 30 Euro atau (Rp 497ribu) per bulan.

Aplikasi Financial Malware



- *Financial malware* adalah *malware* yang dirancang khusus untuk mencuri kredensial atau melakukan serangan *man-in-the-middle* pada aplikasi finansial. *Financial malware* mungkin merupakan *keylogger* yang mengumpulkan nomor kartu kredit, atau mungkin lebih canggih dan mencegat kode autentikasi SMS untuk menyerang aplikasi e-banking.
- Proses *financial malware* dijalankan dalam 3 langkah :
 1. Menginfeksi sistem *smartphone*.
 2. Mengambil data finansial dengan serangan *man-in-the-middle* pada transaksi perbankan.
 3. Melakukan transaksi perbankan menggunakan kredensial yang dicuri.
- Sebagai contoh:
 1. ZeuS Mitmo yang menggabungkan vektor serangan SMS dan website untuk menargetkan bank *online* melalui *smartphone*.
 2. File APK (Android Package Kit) yang dikirimkan melalui *phishing*.



Aplikasi Financial Malware



Tahapan phishing berkedok undangan pernikahan



INVESTIGATE

Penjahat siber membuat file APK yang dinamai sebagai undangan pernikahan atau tautan (link) untuk men-download file APK



Penjahat siber menghubungi korban dan mendesak korban untuk segera membuka file undangan pernikahan dan meng-install file APK pada smartphone Android



PLAY

Setelah file APK berhasil ter-install, maka penjahat siber segera membobol rekening atau dompet digital milik korban



EXIT

Setelah itu, penjahat siber mengakhiri komunikasi dengan cara yang natural, sehingga korban tidak curiga



Bismillahirrahmanirrahim

Kepada teman-teman sekalian,
sebelumnya saya meminta maaf
karena mengabarkan berita bahagia
ini hanya dengan lewat pesan
singkat.

Merupakan suatu kehormatan bagi
kami apabila ERNAWATI, dapat
menghadiri prosesi Pernikahan
kami pada Undangan dibawah ini

18.44

Pesan ini telah dihapus 18.44

Di buka undangan nya buk di tunggu
kehadiran nya 😊 18.50

18.50

punten ieu sareng saha abdi teu kenal
19.13 ✓

Bu di buka undangan nya 19.53 SOLOPC

19.53

Sumber gambar:
<https://news.solopos.com/waspada-mulai-marak-begini-modus-penipuan-via-undangan-nikah-di-wa-1537192>



•MODUS OPERANDI PHISHING



Disusun Oleh:



Restia Moegiono
{CEH|CHFI|CSA|QRMO}
Praktisi Keamanan Siber dan
Penggiat Literasi Digital

Instagram dan Tiktok @restiapriw
LinkedIn Restia Moegiono

E-book Modus Operandi Phishing



<https://s.id/ebookmodusphishing>

Aplikasi Mobile Ransomware

- Mobile ransomware adalah bentuk *malware* yang mencuri data sensitif dari *smartphone* atau mengunci perangkat. Kemudian akan meminta tebusan (*ransom*) agar pengguna dapat mendekripsi data pengguna di perangkat, atau tidak membocorkan data sensitif ke publik.
- Terkadang pengguna tertipu untuk mengunduh mobile ransomware secara tidak sengaja melalui unduhan konten yang seolah-olah aman atau software yang penting.
- Setelah *malware* diunduh ke *smartphone*, *malware* akan menampilkan pesan palsu yang menuduh pengguna melakukan perbuatan yang melanggar hukum sebelum mengenkripsi file dan mengunci data di *smartphone*.
- Pembayaran *ransomware* seringkali melalui mata uang kripto (*cryptocurrency*) Bitcoin, kemudian penjahat *ransomware* akan mengirimkan kode untuk membuka *smartphone* atau mendekripsi data. Namun , membayar *ransomware* tidak disarankan.

Aplikasi Mobile Ransomware

a video by



Serangan Phising



Phishing adalah serangan *social engineering* secara *online*, yang memancing korban untuk mengungkapkan data yang sensitif/rahasia (mengarahkan korban ke situs buatan penjahat siber berupa form) atau memasang perangkat lunak berbahaya/malware (meng-klik tautan berbahaya atau men-download file) yang dapat melakukan pencurian data. *Phishing* awalnya menggunakan media komunikasi *email*.



Phishing melalui pesan *SMS/pesan chat (smishing)* adalah penipuan *phishing* melalui media komunikasi *SMS/pesan chat*. Pesan yang dikirimkan melalui *SMS/pesan chat* di *smartphone* terasa lebih personal sehingga membuat korban kurang waspada. Modusnya serupa dengan *phishing* melalui *email*.



Phishing melalui *telepon (vhishing)* adalah penipuan *phishing* melalui media komunikasi *telepon*. Modusnya yaitu memancing korban untuk mengungkapkan data yang sensitif/rahasia (menyebutkan data yang sensitif/rahasia) atau mendesak korban untuk mentransfer sejumlah uang.

Apa itu *Social Engineering*?



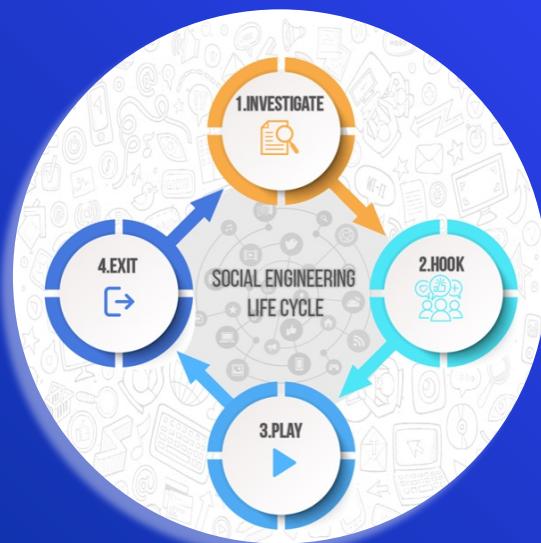
Social engineering (rekayasa sosial) adalah teknik manipulasi psikologis manusia yang digunakan agar korban melakukan tindakan tertentu yang merugikan, seperti mengungkapkan informasi/data rahasia, menginstal *malware*, sampai mentransfer sejumlah uang.



Social engineering memanfaatkan cara kerja otak manusia dan sifat-sifat naluriah manusia.

Siklus pada Serangan Social Engineering

001



(1) **Investigate** : mempersiapkan serangan social engineering

- Mengidentifikasi calon korban di internet
- Mengumpulkan informasi profil calon korban di media sosial
- Memilih metode serangan social engineering

(2) **Hook** : mendapatkan pijakan awal untuk menipu korban

- Mulai melibatkan calon korban melalui media komunikasi online/tatap muka
- Memutar balikkan cerita yang sebenarnya untuk mengelabuhi korban
- Mengambil kendali interaksi (dominan) terhadap korban

(3) **Play** : menjalankan tindakan yang merugikan korban

- Memperluas pijakan yang digunakan untuk menipu korban
- Mendesak korban untuk melakukan hal-hal yang merugikan seperti mengungkapkan informasi/data rahasia, menginstal malware, sampai mentransfer sejumlah uang
- Melakukan tindakan yang merusak, seperti membuat gangguan layanan TI, mengekstraksi data ke luar sistem elektronik (kebocoran data)

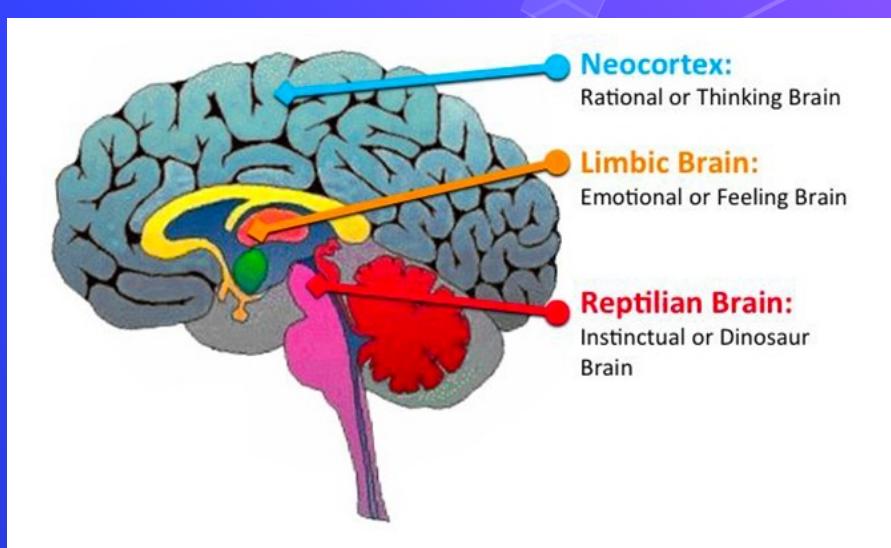
(4) **Exit** : menutup interaksi secara natural tanpa menimbulkan kecurigaan korban

- Menghapus semua jejak malware yang digunakan
- Menutupi jejak interaksi
- Membawa sandiwara ke akhir yang natural dan mengakhiri komunikasi

Bagaimana Social Engineering Terjadi?

Tiga bagian otak manusia terdiri dari:

1. **Batang atau otak reptil**: berkaitan dengan insting mempertahankan hidup dan dorongan untuk mengembangkan spesies.
2. **Sistem limbik atau otak mamalia**: fungsi proses penyimpanan perasaan manusia, pengalaman yang menyenangkan, memori, dan kemampuan belajar manusia.
3. **Neokortex**: mengatur pesan yang diterima oleh panca indera, merupakan sistem kecerdasan tertinggi manusia, yang diiringi kemampuan untuk menerima atau menolak terkait dengan informasi yang kita terima.



Social Engineering memanfaatkan sifat-sifat naluriah manusia sebagai trigger terhadap cerita yang diputarbalikkan faktanya: ketakutan, rasa ingin tahu, keinginan untuk membantu, kecenderungan untuk percaya, kemalasan, ketamakan.

Tanda-Tanda Serangan Social Engineering



'Teman' Anda mengirim Anda pesan yang aneh

Jika Anda tiba-tiba menerima pesan yang aneh atau tidak biasanya dikirimkan oleh teman, maka berhati-hatilah karena mungkin akunnya kena hack.



Emosi Anda tiba-tiba meningkat

Jika Anda tiba-tiba emosional, seperti marah, menangis, ketakutan setelah menerima pesan, maka berhati-hatilah.



Ada permintaan yang sangat mendesak

Jika ada permintaan yang segera, jika tidak dilakukan maka berhati-hatilah.



Ada tawaran itu terasa terlalu bagus untuk menjadi kenyataan

Jika Anda menerima tawaran yang sangat menggiurkan, sementara Anda tidak pernah mengusahakan apapun. Maka berhati-hatilah.



Ada bantuan yang tidak pernah Anda minta

Bantuan biasanya diberikan berdasarkan permintaan. Jika ada bantuan yang tidak pernah diminta, maka berhati-hatilah.



Orang yang berkomunikasi dengan Anda tidak dapat membuktikan identitasnya

Jika Anda komunikasi online, namun mengenali dan memastikan identitas orang lain yang Anda ajak berkomunikasi (autentikasi). Maka berhati-hatilah.

001

010

Cara Mengatasi Phising

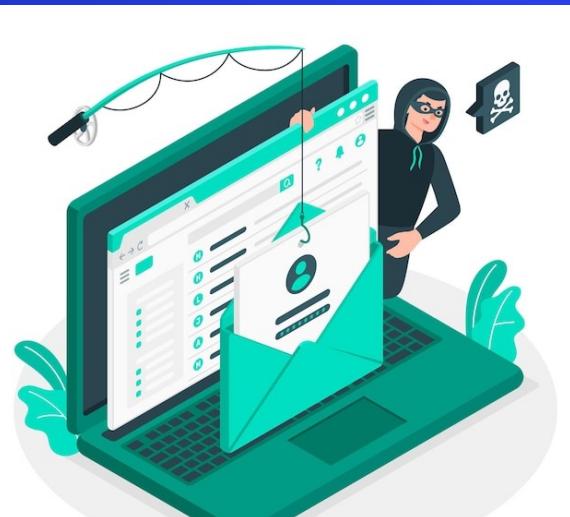
1. Menerapkan Metode STARR



- **STOP** : Berhenti sejenak agar kamu tidak larut dalam emosi negatif/emosional yang muncul, sehingga dominan di otak reptil dan otak mamalia.
- **THINK** : Berpikir pada kondisi jernih ketika emosi sudah mereda dengan menggunakan otak neokorteks akan mengatasi serangan *social engineering*.
- **ASSESS** : Menilai emosi yang dirasakan secara objektif dan rasional berdasarkan informasi yang diterima akan mengatasi serangan *social engineering*.
- **RESPOND** : Memberikan respon yang tepat dan cepat dengan prinsip bijak, adil dan berani akan mengatasi serangan *social engineering*.
- **REVIEW** : Reviu terhadap tindakan yang dilakukan pada serangan *social engineering* akan memberikan wawasan untuk pencegahan serangan serupa di kemudian hari.

Cara Mengatasi Phising

2. Mampu Mendeteksi *Email Phishing*



Menemukan *email phishing* berarti bisa mendeteksi adanya sesuatu yang tidak konsisten atau tidak biasa. Terkadang sulit untuk mengenali apa yang asli dan apa yang merupakan upaya *phishing*, terlebih dengan adanya *Artificial Intelligence* (AI) seperti ChatGPT. Berikut adalah tanda-tanda *email phishing* :

- a. Lampiran atau tautan yang mencurigakan.
- b. Tata bahasa yang buruk : typo, kesalahan ejaan.
- c. Grafik (gambar) tidak profesional : buram, ukuran terlalu besar/kecil
- d. Urgensi yang tidak perlu untuk memverifikasi alamat *email* Anda atau informasi pribadi lainnya dengan segera.
- e. Salam umum seperti "Pelanggan yang Terhormat", tidak menggunakan mengunakan nama Anda. Artinya pesan dikirim secara *random*.



Cara Mengatasi Phising

3. Mampu Menganalisis Email Phishing

The screenshot shows an email inbox with a message from Barbora Ondrikova. The message subject is "Slido call". The email content includes a greeting, a request for feedback, and a statement about noticing the recipient's use of Slido. A yellow box labeled '1' highlights the three-dot menu icon in the top right corner of the message preview. A red circle highlights the same icon.

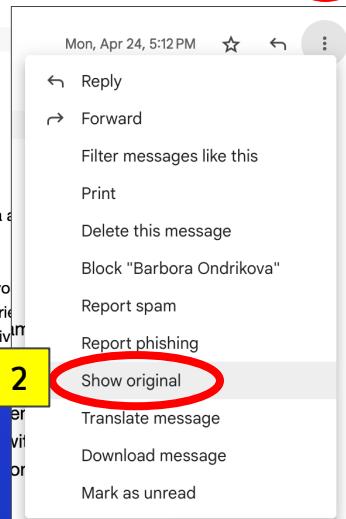
Mon, Apr 24, 5:12 PM 22 of 140

Barbora Ondrikova <bondrikova@slido.com> Unsubscribe to me

slido

Hello there!

I hope this email finds you well. My name is Barbora and I am truly interested in hearing about your experience with our product. Your feedback is invaluable to us as we strive to improve and make Slido even better for you.



Original Message

Message ID <30178436.20230424101254.6446562670c907.40068867@mail179-13.suw41.mandrillapp.com>

Created at: Mon, Apr 24, 2023 at 5:12 PM (Delivered after 0 seconds)

From: Barbora Ondrikova <bondrikova@slido.com>

To: rmoegjono@gmail.com

Subject: Slido call

SPF: PASS with IP 198.2.179.13 [Learn more](#)

DKIM: 'PASS' with domain slido.com [Learn more](#)

DMARC: 'PASS' [Learn more](#)

[Download Original](#)



[Copy to clipboard](#)

4. Masuk ke : [The screenshot shows the MXToolbox "Email Headers" analysis page. A red circle highlights the "Copy/Paste Warning" section. Another red circle highlights the "Header Analyzed" section, which lists several green checkmarks indicating compliance with various email standards. MX TOOLBOX Pricing Tools Delivery Center Monitoring Products Support Login SuperTool MX Lookup Blacklists DMARC Diagnostics Email Health DNS Lookup Analyze Headers All Tools **Copy/Paste Warning** There is a known problem with copy/pasting headers from messages. Sometimes, this causes the format of the message to change and will cause DKIM to fail. Download the eml file, open it in a text editor and copy from there or use our \[Email Deliverability Tool\]\(#\). Please see our guide for using GSuite/Gmail headers **Header Analyzed** Email Subject: =?utf-8?Q?Slido=20call?= **Delivery Information** - ✓ DMARC Compliant - ✓ SPF Alignment - ✓ SPF Authenticated - ✓ DKIM Alignment - ✓ DKIM Authenticated 5](https://mxtoolbox.com>EmailHeaders.aspx</h2></div><div data-bbox=)

Cara Mengatasi Phising

4. Mampu Mengatasi *Email Phishing*



Hapus *email* tanpa membukanya

Sebagian besar virus aktif saat Anda membuka lampiran (*attachment*) atau mengklik tautan di dalam *email*. Tetapi beberapa aplikasi *email* mengizinkan pembuatan skrip yang memungkinkan untuk terkena virus hanya dengan membuka *email* yang tampak mencurigakan. Cara yang terbaik adalah menghindari membuka *email phishing* tersebut.



Blokir pengirim secara manual

Jika aplikasi *email* Anda mengizinkan Anda melakukan blokir secara manual, Anda harus melakukannya. Catat domain *email* pengirim, lalu tambahkan pengirim ke daftar yang diblokir. Ini bermanfaat jika Anda mengakses *inbox email* secara bersama-sama untuk menghindari rekan yang lain membuka *email phishing* secara tidak sengaja.



Beli aplikasi antivirus

Anda mungkin tidak pernah bisa benar-benar aman. Pertimbangkan untuk membeli perangkat lunak antivirus yang dapat membantu memantau *inbox email* Anda.

Cara Mengatasi Phising

5. Mampu Mengatasi Phishing Melalui SMS atau pesan chat



Menolak untuk memberikan umpan balik (feedback) atau tidak menanggapi. Kalau perlu blokir kontak.



Anda harus menganggap peringatan keamanan yang mendesak dan penukaran kupon, atau penawaran yang harus Anda lakukan dengan segera sebagai tanda peringatan (warning) terhadap upaya peretasan.



Tidak ada lembaga keuangan atau situs belanja *online* yang akan mengirimkan SMS yang meminta Anda untuk memperbarui informasi akun Anda atau mengonfirmasi kode kartu ATM Anda. Jika Anda mendapatkan pesan yang tampaknya berasal dari bank atau situs belanja *online*, dan meminta Anda untuk meng-klik *link* atau *men-download file* dalam pesan tersebut, maka itu adalah penipuan. Hubungi bank atau situs belanja *online* pada kontak resmi untuk mengkonfirmasi.



Jangan pernah meng-klik tautan atau *men-download file* dalam pesan yang dikirimkan teman yang dikenal, sebelum melakukan autentikasi lebih detail/menggunakan media komunikasi lain/tatap muka. Bisa jadi akun tersebut sudah di-hack.

Cara Mengatasi Phising

6. Mampu Mengatasi Phishing Melalui SMS atau pesan *chat*



Hindari kontak dengan nomor mencurigakan:

- Nomor layanan, seperti "5000" karena nomor-nomor ini teraut ke layanan email-to-text, yang terkadang digunakan oleh penjahat siber untuk menghindari memberikan nomor telepon mereka yang sebenarnya.
- Nomor telepon dengan kode negara lain yang diduga tidak memiliki registrasi nomor yang ketat, seperti : (+91: India), (+234: Nigeria), (+48: Polandia).



Laporkan semua serangan *phishing* melalui SMS/pesan *chat* ke Kominfo yang memiliki layanan pengaduan untuk mencoba melindungi orang lain melalui situs <https://aduannomor.id>

Cara Mengatasi Phising

7. Mampu Mengatasi Phishing Melalui Telepon (Whishing)



Jangan menjawab panggilan telepon dari nomor yang tidak dikenal

Sangat menggoda untuk menjawab panggilan dari nomor yang tidak dikenal. Anda bahkan mungkin berpikir, 'Bagaimana jika ini keadaan darurat dan seseorang membutuhkan saya?' Ketahuilah bahwa siapa pun yang menelepon Anda dengan keadaan darurat akan meninggalkan pesan.



Jangan menyerah pada tekanan

Jika seseorang mencoba memaksa Anda untuk memberi mereka informasi sensitif, tutup telepon dan kalau perlu blokir nomornya.



Tidak tertarik dengan tawaran yang terlalu bagus untuk menjadi kenyataan

Inginlah selalu tawaran yang terlalu bagus untuk menjadi kenyataan, bisa jadi adalah upaya phishing. Oleh karena itu, Anda harus berhati-hati.

Cara Mengatasi Phising

8. Mampu Mengatasi Phishing Melalui Telepon (*Vhishing*)



Tetap Tenang dan Jangan Panik

Karena penjahat ini sering mempermainkan emosi Anda, tetap tenang dan tutup telepon (metode STARR). Jika Anda masih merasa takut, tunggu 10 menit lalu hubungi bank Anda, perusahaan kartu kredit, atau siapa pun yang mengaku sebagai penelepon untuk memverifikasi apakah ada masalah.



Laporkan

Laporkan semua serangan *vhishing* ke Kominfo yang memiliki layanan pengaduan untuk mencoba melindungi orang lain melalui situs <https://aduanomor.id>.

Cara Mengatasi Phising

9. Mengaktifkan Two-Factor Authentication

Terdapat beberapa cara untuk melakukan two-factor authentication, yaitu:

a. SMS

Autentikasi ini menggunakan jaringan GSM untuk mengirimkan *One Time Password* (OTP), jadi pastikan smartphone bisa menerima SMS dengan mudah.

b. Whatsapp

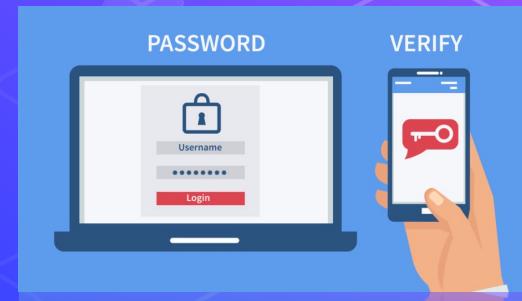
Autentikasi ini menggunakan aplikasi Whatsapp untuk mengirimkan OTP.

c. Aplikasi authentication

Autentikasi ini menggunakan aplikasi yang akan membangkitkan OTP. Terdapat beberapa aplikasi yang bisa digunakan, misalnya aplikasi Duo Mobile dan Google Authenticator.

d. Hardware security key

Autentikasi ini menggunakan hardware sebagai security key atau security token, misalnya Yubikey authenticator.



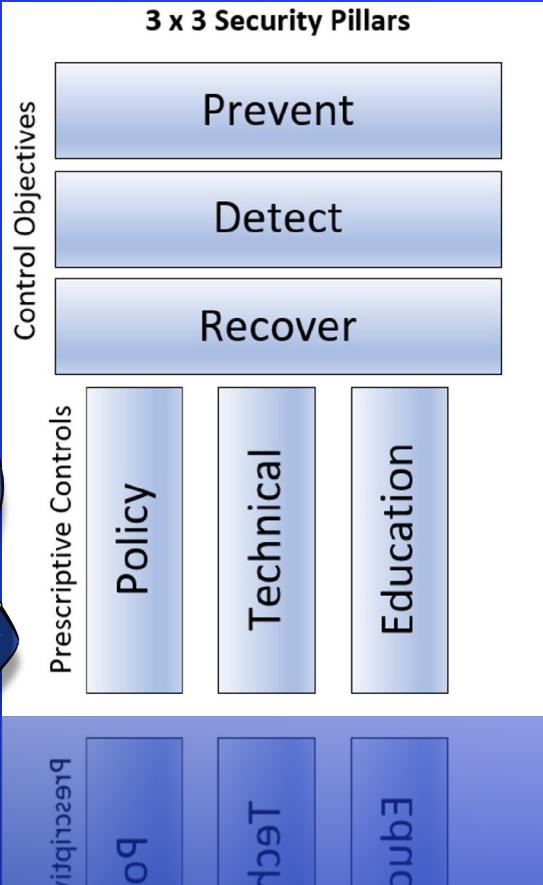
Catatan:

Amankan *recovery code* yang diperlukan sebagai metode autentikasi *backup* jika metode *two-way authentication* gagal.

Bagaimana MFA Dapat Mengatasi Phishing?



Penanganan Phishing pada Organisasi



Organisasi harus menerapkan kombinasi terbaik dari kebijakan keamanan, kontrol keamanan teknis, dan edukasi untuk mengurangi risiko phishing pada organisasi:

1. Kebijakan keamanan

Kebijakan keamanan adalah instruksi, rekomendasi, dan prosedur yang efektif, konsisten, dan dikomunikasikan di organisasi untuk mengurangi risiko keamanan secara efektif.

2. Kontrol Keamanan teknis

Kontrol keamanan teknis adalah semua mitigasi dan kontrol fisik dan logis yang diterapkan untuk mencegah sesuatu yang berbahaya terjadi pada perangkat keras, sistem operasi, dan aplikasi.

3. Edukasi

Pelatihan security awareness adalah semua tindakan yang dilakukan untuk membuat orang sadar terhadap dampak serangan social engineering termasuk phishing, membantu mengenali ancaman dan mengambil tindakan yang tepat.

Ciri-ciri Smartphone Terkena Serangan Siber

1. Penggunaan baterai smartphone yang boros

Buka *Settings > Battery > Battery Usage* untuk mengetahui aplikasi apa saja yang berperan dalam penggunaan baterai.

2. Terdapat aplikasi tidak dikenal ter-install di smartphone

Buka *Settings > Apps > App Manager* dan carilah apakah ada aplikasi tidak dikenal yang sudah ter-install di smartphone?

3. Penggunaan data yang tinggi pada smartphone

Buka *Settings > Connections > Mobile Data Usage* atau *WiFi Data Usage* untuk memeriksa aplikasi yang menggunakan data. Amati, apakah ada yang tidak normal?

4. Terdapat iklan dan pop-up yang aneh di smartphone

Amati smartphone apakah ada iklan atau pop-up yang aneh? Jika ada, jangan pernah di-klik!

5. Aplikasi dan smartphone sering lambat

Jika smartphone seringkali lambat tanpa alasan yang bisa dijelaskan, bisa jadi karena smartphone sudah diretas.



Ciri-ciri Smartphone Terkena Serangan Siber

6. Pengguna menerima tagihan telepon yang mahal: tanda-tanda dari *diallerware*.
7. Terdapat **toolbar**, **search engine**, dan halaman **home internet baru** yang pengguna tidak ingat kapan pernah memasangnya.
8. Kesulitan masuk ke situs yang aman: tanda-tanda dari *financial malware*. Jika upaya *login* pertama gagal dan yang kedua berhasil, itu mungkin berarti upaya pertama dilakukan pada browser palsu dan password telah dikomunikasikan ke pihak ketiga, bukan ke bank pengguna.
9. Aplikasi antivirus dan perangkat lunak keamanan lainnya tidak berfungsi.
10. Pada Android, bagian **Settings>Security**, pengaturan "**Unknown Sources**" diaktifkan: memungkinkan aplikasi yang tidak ada di Google Play Store dapat diunduh dan diinstal. Jika pengaturan ini telah diaktifkan, maka merupakan pertanda potensial bahwa *malware* mungkin telah diinstal secara tidak sengaja.
11. Pada iPhone, terdapat aplikasi bernama **Cydia**: yang memungkinkan pengguna menginstal perangkat lunak pada smartphone yang sudah di-jailbreak. Jika ada dan pengguna tidak merasa sudah menginstalnya, segera hapus.
12. **Smartphone telah berhenti menerima pembaruan ke versi terbaru meskipun kompatibel**.

Cara Mencegah Serangan Siber pada Smartphone

1. Perbarui sistem operasi dan software

Patch keamanan reguler pada pembaruan sistem operasi dan perangkat lunak dapat membantu memperbaiki kerentanan yang dapat digunakan hacker untuk masuk ke smartphone.

2. Berhati-hati terhadap serangan phishing

Phishing bisa terjadi melalui *email* dan situs web yang terlihat mencurigakan atau bahkan terlihat terlalu bagus untuk menjadi kenyataan (*too good to be true*). Malware dapat masuk ke smartphone melalui unduhan yang secara tidak sengaja ketika mengunjungi situs web yang disusupi.

3. Berhati-hatilah saat memasang aplikasi

Aplikasi palsu adalah sumber *malware* yang terkenal, yaitu aplikasi yang terlihat sah padahal berbahaya. Sebelum memasang aplikasi, pastikan Anda mengunduhnya dari toko aplikasi resmi, seperti App Store atau Google Play. Toko aplikasi yang diberikan oleh pihak ketiga sangat berisiko.

4. Back up semua data

Mem-back up data di smartphone selalu merupakan ide yang bagus. Hal ini akan sangat bermanfaat ketika data smartphone tidak bisa diakses karena smartphone terkena *ransomware*, atau ketika pengguna kehilangan smartphone.

Cara Mencegah Serangan Siber pada Smartphone

5. Gunakan solusi keamanan smartphone yang tangguh

Menjaga semua perangkat terlindungi dengan solusi keamanan yang komprehensif sangat disarankan. Aplikasi keamanan smartphone dapat berupa aplikasi mobile antivirus, mobile Endpoint Detection and Response (EDR), Mobile Device Management (MDM), dan aplikasi sejenis lainnya.

6. Jangan berikan hak akses kepada siapa pun yang tidak berhak

Pada smartphone jangan biarkan orang lain memegang hak akses, meski dia terlihat baik sekalipun. Berusahalah untuk tidak mudah mempercayai orang lain. Dengan memberikan hak akses pada smartphone akan memberikan peluang untuk menginstal malware.

7. Tidak memasang aplikasi tidak resmi

Jauhkan malware dari smartphone dengan memastikan telah menerapkan pengaturan yang melarang pemasangan aplikasi tidak resmi pada Settings>Security, kemudian hapus centang pada "Unknown Sources".

8. Pasang kunci layar (*screen lock*) pada smartphone

Hal ini bertujuan untuk mencegah akses yang tidak sah pada smartphone yang memungkinkan dilakukan instalasi malware.

Cara Mencegah Serangan Siber pada Smartphone

9. Tetap terinformasi tentang ancaman terbaru

Varian *malware* terus berkembang, penjahat siber diketahui menggunakan varian *malware* yang diketahui sebelumnya. Semakin banyak yang kita ketahui tentang bagaimana serangan *malware* dilakukan, maka akan semakin mudah dan cepat untuk menemukan solusi.

10. Jangan men-root atau men-jailbreak smartphone

Hal ini akan membuka peluang smartphone terinfeksi terhadap *malware*. Tindakan ini sangat tidak disarankan, kecuali pengguna benar-benar membutuhkan fungsionalitas tertentu dengan men-root atau men-jailbreak smartphone.

11. Batasi hak administrator di aplikasi smartphone

Pastikan hanya aplikasi khusus yang diperbolehkan memiliki hak administrator seperti aplikasi antivirus.

12. Perhatikan izin (permission) yang diberikan kepada aplikasi

Perhatikan aplikasi yang meminta izin untuk mengakses mikrofon, kamera, telepon, atau data pribadi. Jika aplikasi menginginkan lebih banyak informasi daripada yang tampaknya masuk akal, misalnya, game Sudoku yang menginginkan akses ke kamera maka itu mungkin merupakan tanda muatan spyware.

Cara Mencegah Serangan Siber pada Smartphone

13. Jangan men-download konten bajakan

Konten bajakan seringkali digunakan para penjahat siber untuk menyebarkan malware. Pengguna harus dapat mengendalikan keinginannya untuk mengunduh konten bajakan dan hindari potensi bencana.

14. Selalu pantau laporan transaksi yang dilakukan aplikasi mobile banking

Financial malware berpotensi melakukan transaksi tidak sah. Oleh karena itu, penting untuk pengguna bisa mendeteksi adanya transaksi tidak sah dengan memantau laporan transaksi.

15. Selalu log out setelah selesai transaksi

Financial malware berpotensi melakukan transaksi tidak sah dengan memanfaatkan sesi (session) yang masih aktif. Oleh karena itu, penting untuk melakukan *log out* setelah selesai transaksi di aplikasi mobile banking.

16. Aktifkan autentikasi dua faktor

Jika akun *online* memiliki opsi *two factor authentication* (2FA), maka pengguna disarankan untuk mengaktifkan opsi ini untuk menambah langkah verifikasi ketika terjadi *login* baru.

17. Gunakan password yang kuat

Password yang kuat terdiri atas kombinasi huruf besar, huruf kecil, angka dan simbol dengan panjang minimal 8 (delapan) karakter, serta harus diganti secara berkala.

Penanganan Serangan Siber pada Smartphone (Kasus File Trojan APK)

1. Segera lakukan *flight mode* (mode terbang) diaktifkan agar koneksi ke penjahat siber dengan smartphone terputus.
2. Backup file-file penting (misalnya video dan gambar serta dokumen).
3. Lakukan *factory reset*. Setelah selesai, smartphone akan tampak seperti baru lagi.
4. Registrasi pada smartphone dengan akun gmail untuk Android atau Apple ID untuk iPhone.
5. Install aplikasi antivirus, kemudian jalankan *scanning* awal untuk memastikan tidak ada lagi ancaman siber (misalnya *malware*).
6. Install kembali aplikasi Whatsapp, kemudian aktifkan biometrik sebagai proteksi agar aplikasi tidak bisa dibajak oleh penjahat siber. Sebagian Trojan APK mentargetkan aplikasi Whatsapp untuk penyebaran *malware*-nya.
7. Aktifkan juga *screenlock* biometrik seperti *fingerprint* atau *face* untuk proteksi hak akses ke smartphone.



Referensi

- Mobile Device Security – Goldphish (<https://www.youtube.com/watch?v=PTXnMRG8NEw>)
- Gambar (<https://www.freepik.com/>)
- The impact of a phishing attack. (<https://www.phriendlyphishing.com/blog/the-impacts-of-a-phishing-attack>)
- E-Book Comprehensive Anti-Phishing Guide by KnowBe4
- All About Phishing Scams & Prevention: What You Need to Know (<https://www.kaspersky.com/resource-center/preemptive-safety/phishing-prevention-tips>)
- What is Smishing and How to Defend Against it? (<https://usa.kaspersky.com/resource-center/threats/what-is-smishing-and-how-to-defend-against-it>)
- What is Vishing? Voice Phishing Scams Explained & How to Prevent Them (<https://fraudwatch.com/what-is-vishing-voice-phishing-scams-explained-how-to-prevent-them/>)
- Mengendalikan Emosi ala Filosofi Teras (<https://www.bobobox.co.id/blog/mengendalikan-emosi-a-la-filosofi-teras/>)
- Kuliah Digital Ramadhan 1445 H by Muhammad Nuh Al-Azhar.