

# PHISING: UMPAN MANIS, BAHAYA SADIS!



BERKAH RAMADHAN

Selamat! No.anda

Resmi M-dpt hadiah

Cek Rp.100jta

Dri PT.M-KIOS

PIN:2159CRT51

hub:[082291311157](tel:082291311157)

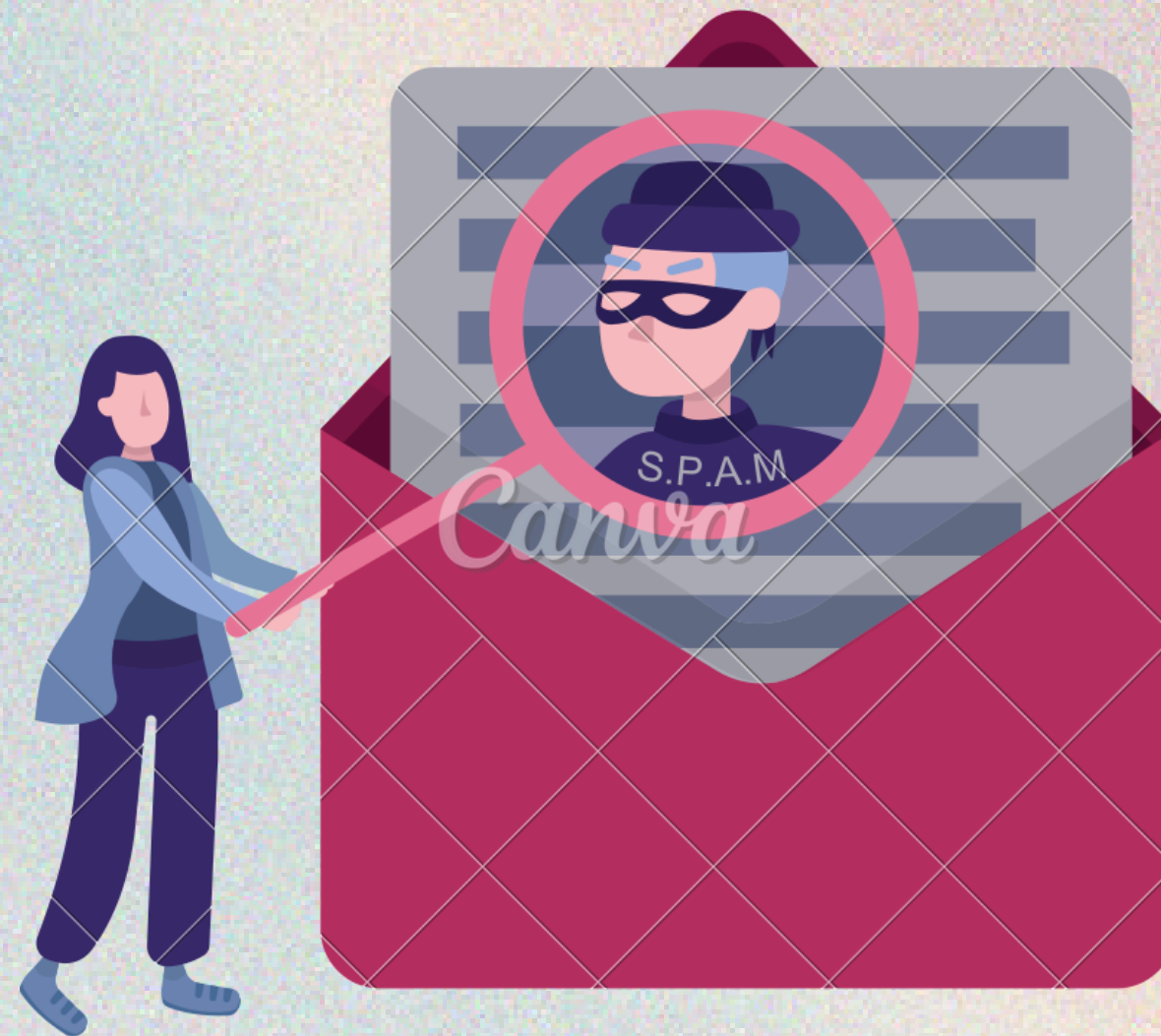
U/Info klik:

[www.promoramadhan27.blogspot.com](http://www.promoramadhan27.blogspot.com)



Literasi Media dan Informasi

# PRETEST ANTI-PHISNG







**Literasi Media dan Informasi**

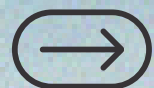
**KLIK LINK DIBAWAH UNTUK KE  
HALAMAN QUIZ**

**QUIZ**

# APA SIH PHISING ITU?

Pencurian informasi pribadi dan data sensitif korban dengan mengirimi mereka pesan, email, atau komunikasi digital lainnya.

Dilakukan dengan mengirimkan email phishing, dokumen berbahaya, ataupun pesan instan yang mencurigakan dimana pelaku akan berpura-pura menjadi suatu entitas yang biasanya dikenal.





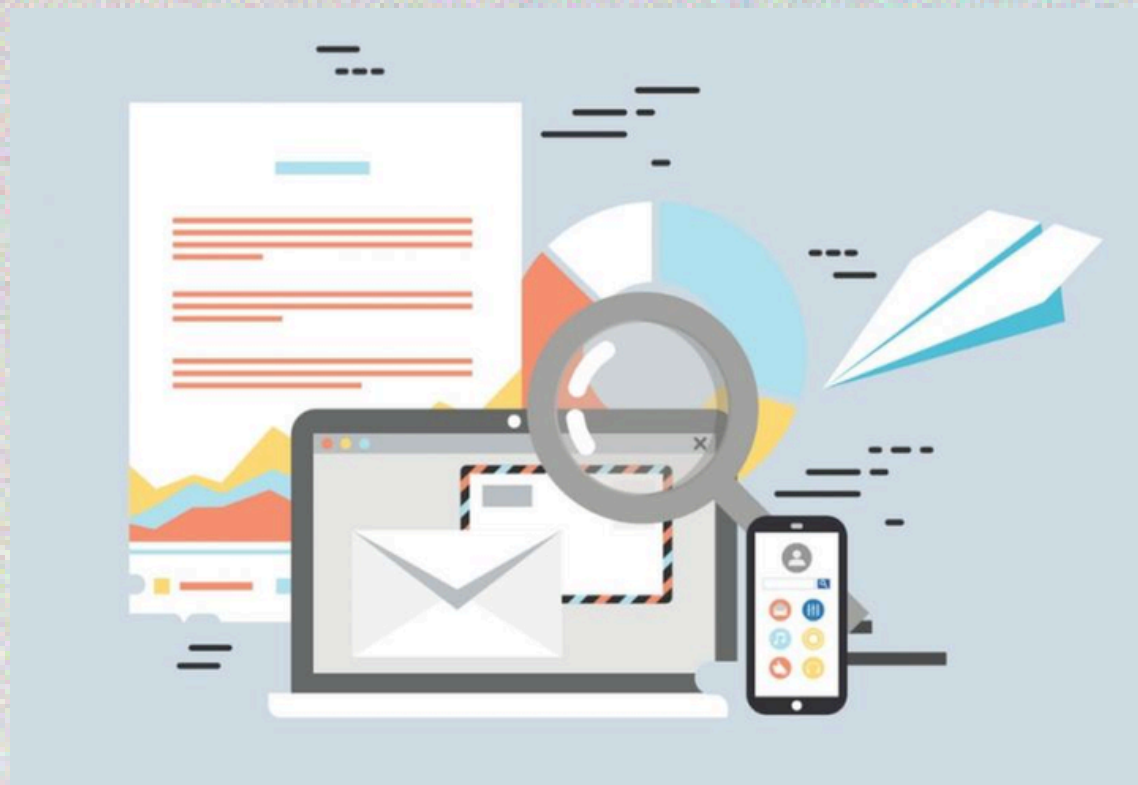
# PHISING BAGI PELAKU

Tujuan dari phising adalah untuk memperoleh informasi penting dari korbannya secara diam-diam, lalu menggunakan informasi tersebut untuk keuntungan pribadi pelaku

Mencuri Uang, Mencuri Identitas, Menyebarkan Malware, ataupun Pemerasan Secara Online



# CONTOH-CONTOH PHISING



## ● EMAIL JEBAKAN

Pelaku kirim email yang kelihatan resmi (kayak dari bank atau kantor), tapi itu palsu. Di dalamnya ada link atau file yang kalau dibuka, bisa bikin data anda dicuri.

## ● EMAIL JEBAKAN TAPI KHUSUS BUAT TERGETNYA

Mirip email phishing, tapi ini lebih niat. Pelaku cari tahu dulu tentang anda—misalnya nama, kerja di mana, temenan sama siapa—biar jebakannya lebih meyakinkan

## ● SMS PENIPUAN

Pelaku kirim SMS palsu, bilang anda dapat hadiah, akun diblokir, atau paket gagal kirim. Terus dikasih link buat kamu klik.



# CONTOH-CONTOH PHISING



- **TELEPON PENIPUAN**

Pelaku telepon pura-pura jadi CS bank, polisi, atau pegawai kantor penting. Terus minta kode OTP, PIN, atau data lainnya.

- **KETIK ALAMAT WEB BENER, TAPI MASUK KE SITUS PALSU**

ketik alamat asli (kayak klikbca.com), tapi ternyata diarahkan ke situs palsu karena sistemnya udah diretas.

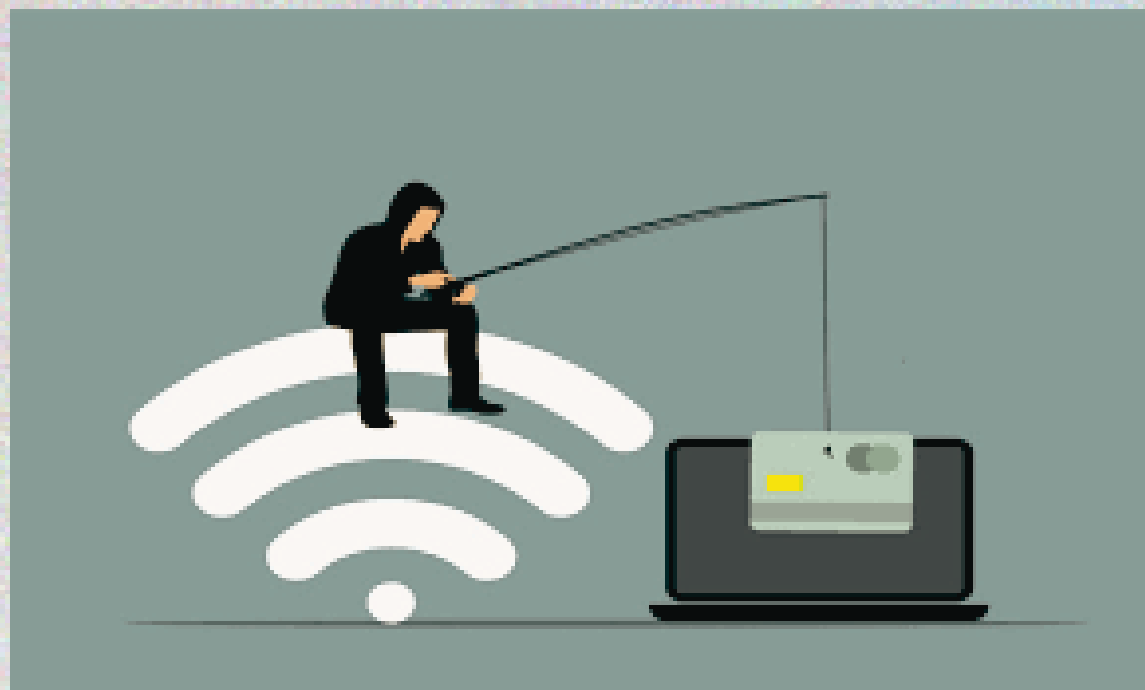
- **SITUS PALSU TAPI KELIHATAN AMAN**

Situs palsu tapi pakai HTTPS dan ada ikon gembok, jadi kelihatan aman padahal nggak. Banyak orang tertipu karena mikir “kalau ada gembok berarti aman”.





# CONTOH-CONTOH PHISING



- **JENDELA IKLAN YANG MINTA DATA PRIBADI**

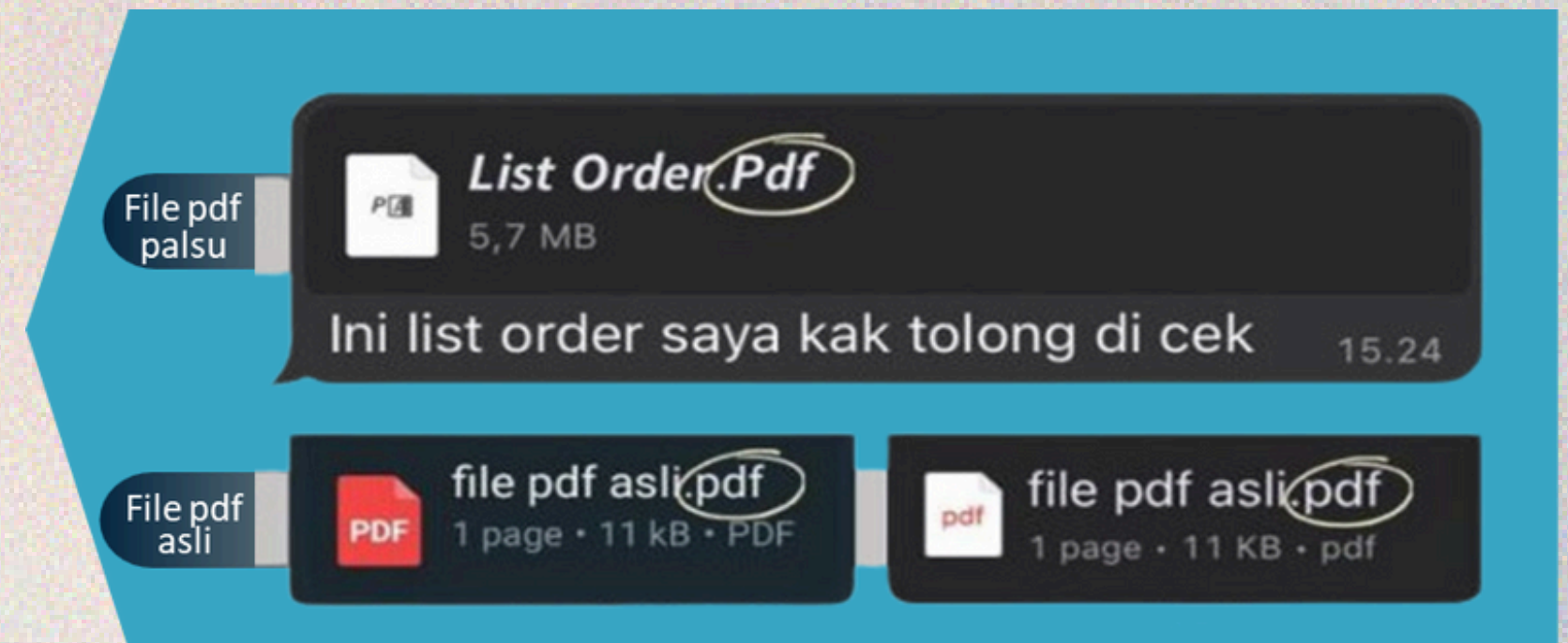
Waktu buka situs, tiba-tiba muncul jendela pop-up minta login, info kartu, atau kode OTP.

- **WI-FI PALSU YANG KELIHATAN ASLI**

Ada Wi-Fi gratisan di tempat umum, tapi itu buatan pelaku. Kalau kamu connect, semua aktivitas kamu bisa disadap



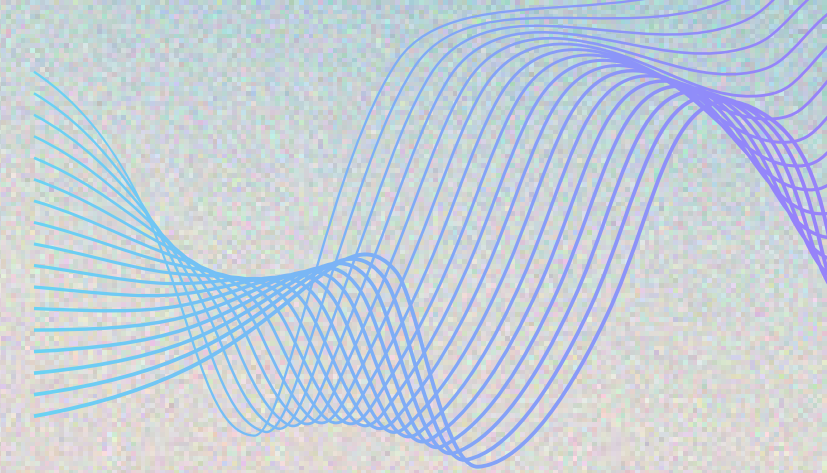




lihat bentuk file yang mencurigakan!







Reply Reply All Forward

IP **Informasi Pajak <info@pajak.gov.id>**  
(External) Pemberitahuan Status Kurang Bayar Pajak

To [Redacted]

Yth. [Redacted]

Sehubungan dengan pelaporan pajak individu tahun 2021 yang wajib Anda laporkan, Anda terhitung mengalami kurang bayar hingga surat ini diterbitkan.

Untuk itu kami menghimbau Anda untuk segera melakukan konfirmasi ulang **NPWP** (Nomor Pokok Wajib Pajak / Data Diri Wajib Pajak) melalui tautan di bawah ini

Bukti Pemotongan Pajak Penghasilan) melalui tautan di bawah ini

[Klik Disini](#)

Jika Anda tidak melakukan konfirmasi hingga tanggal 22 Maret 2022, maka Anda akan dikenakan denda keterlambatan sebesar **100.000 (Seratus Ribu Rupiah)** untuk tiap bulan keterlambatan dan **NPWP** Anda akan dinonaktifkan sementara. Sebagai informasi, untuk NPWP yang tidak aktif mengakibatkan pajak yang wajib dibayarkan tiap bulannya akan menggunakan **tarif pajak tanpa NPWP (20%)** lebih tinggi dari nilai pajak dengan NPWP).

Atas perhatian bapak/ibu, kami ucapkan terima kasih

**djp**  
Direktorat Jendral Pajak  
Jalan Gatot Subroto, Kav. 40-42, Jakarta 12190

**PENIPUAN**

Asalamuaikum nasabah BANK BRI, selamat siang 3.13 PM

**BANK BRI**  
[Pemberitahuan]

Bapak/Ibu Nasabah Yang Terhormat

Sehubungan Adanya Pemberitahuan Dari Layanan Bank BRI Untuk meningkatkan kualitas dan kenyamanan nasabah bertransaksi dan bank bri SMS NOTIFIKASI/BANKING. Mulai nanti malam penggantian hari dan tanggal untuk seluruh biaya transaksi berubah menjadi biaya bulanan. Untuk biaya transaksi yang lama Rp. 550/pertransaksi di ganti dengan biaya yang baru Rp. 150.000/perbulan (Autodebet dari rekening tabungan). Unlimited

Untuk perubahan skema tarif dalam tahap percobaan untuk 6 bulan ke depan dengan ini Kepada Bapak/Ibu Nasabah Bank BRI, untuk Persetujuan, ataupun Konfirmasinya disini Nasabah

1. Apakah Setuju dengan tarif baru perbulan Rp. 150.000. Atau
2. Tidak setuju dan tetap mau menggunakan Tarif Yang Lama Rp. 550 pertransaksi atau perma di kamakan jarang bertransaksi dan untuk Konfirmasi silahkan isi formulir yang di kirimkan. Pastikan semua data di isi semua dengan benar

N.B  
Jika Bapak/Ibu tidak ada Konfirmasi/Maka dianggap setuju. Ada penagihan setiap bulannya Rp. 150.000 dari neg tabungan bri nya ada transaksi atau tidak tetap di potong

15.11

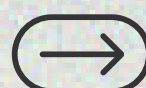
Baik akan kami bantu kembali ketarif normal nya silahkan isi data fromulir nya dengan benar 15.11

Nasabah bank BRI Yang terhormat Untuk komfirmasi Tarif Transaksi anda silahkan klik di bawa ini / Terimakasih <http://perubahantarifbri6500.co> 15.11

Silakan di klik link yang telah kami sediakan ya bapak/ibu dan itu akan langsung mengarahkan bapak/ibu kek formulir untuk pengaktifan tarif nya 🙏 15.11

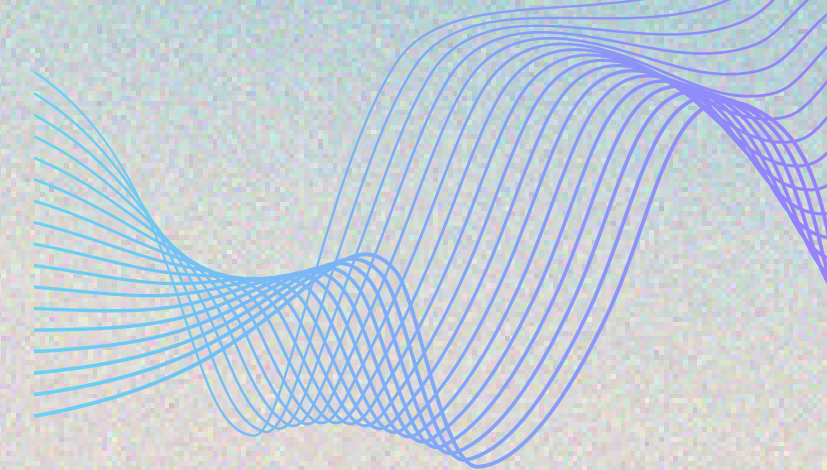
Jika sudah di isi tolong konfirmasi lagi ke kami 😊🙏 15.12

email pajak asli "informasi@pajak.go.id"  
atau cek di google

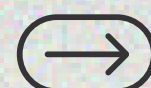


Bank tidak pernah meminta data pribadi nasabahnya





cek kebenarannya terlebih dahulu, jangan asal klik link!



**Situs Resmi**

 <https://www.perusahaan.com>

**Situs Palsu**

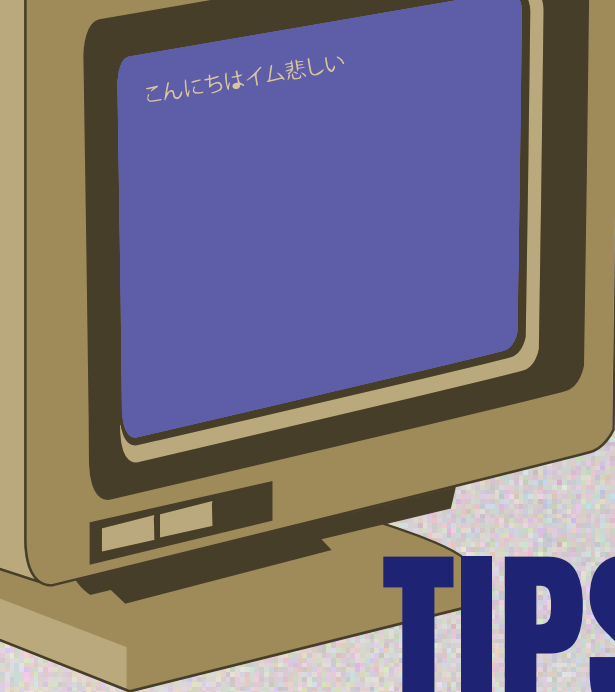
 <http://www.perusahaaan.com>

Memiliki huruf a lebih banyak dari situs resmi

•Hanya untuk contoh

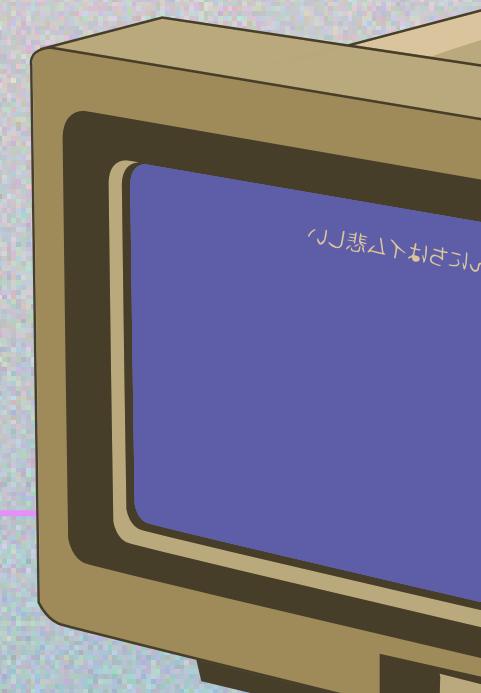
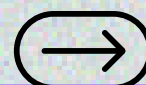
website palsu sangat mirip dengan website aslinya, bahkan terkadang hanya beda satu huruf



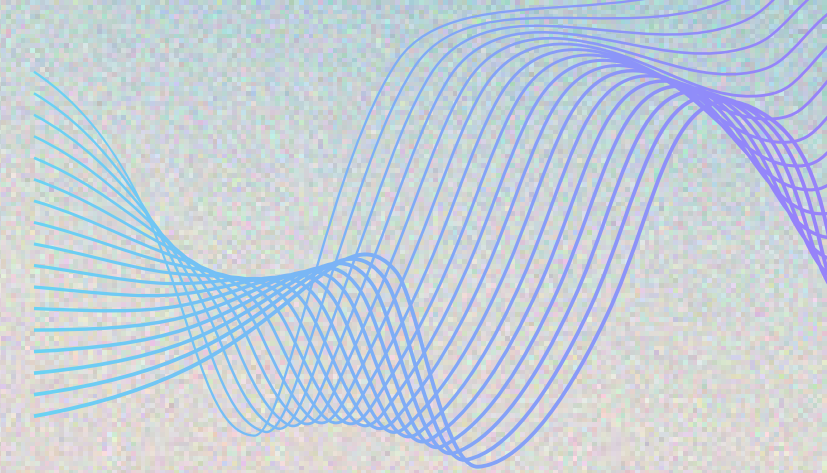


# TIPS MENCEGAH ATAU MENGHINDARI PHISING!

Phishing memang jadi salah satu kejahatan digital yang paling sering terjadi dan merugikan banyak orang. Data pribadi dicuri, akun dibobol, bahkan uang bisa hilang dalam hitungan menit. Tapi tenang—meskipun teknik phishing semakin pintar, kita tetap bisa melindungi diri. Dengan sedikit kewaspadaan dan beberapa kebiasaan aman saat menggunakan internet, kita bisa terhindar dari jebakan para penipu digital ini.







# TIPS MENCEGAH ATAU MENGHINDARI PHISING!

## WASPADAI EMAIL & PESAN YANG MENCURIGAKAN

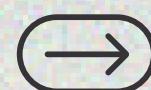
Jangan langsung percaya email, SMS, atau DM yang mendesak atau bikin panik. Periksa alamat pengirim dengan teliti

## CEK ALAMAT WEBSITE (URL) DENGAN TELITI

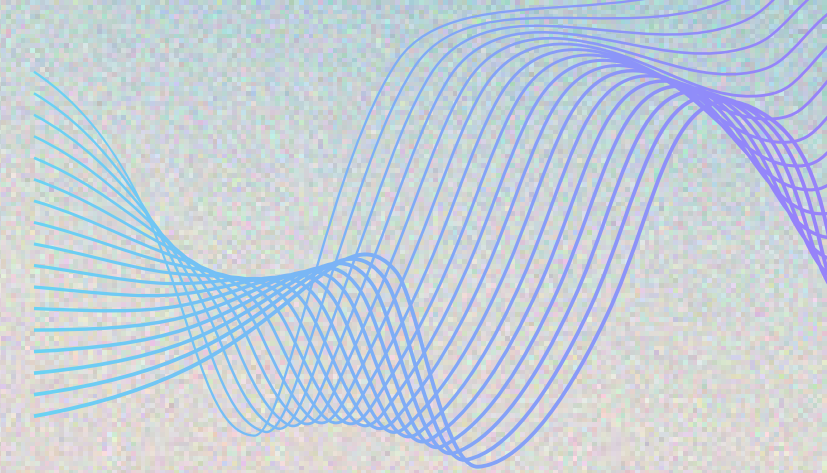
Selalu pastikan situs memiliki URL resmi dan bukan tiruan (contoh: klikbca.com, bukan klikbca.co.com)

## JANGAN BERIKAN INFORMASI PRIBADI LEWAT LINK

Bank, lembaga resmi, atau CS tidak pernah meminta PIN, OTP, atau password lewat SMS, telepon, atau email. Kalau ada permintaan seperti itu, abaikan atau laporkan.







# TIPS MENCEGAH ATAU MENGHINDARI PHISING!

## **GUNAKAN AUTENTIKASI DUA FAKTOR (2FA)**

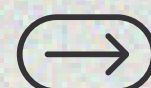
Aktifkan 2FA untuk akun penting seperti email, mobile banking, media sosial, dan e-commerce. Jadi walau password dicuri, akun kamu tetap aman karena butuh kode tambahan

## **SELALU LOG OUT DAN HAPUS JEJAK DIGITAL**

Setelah menggunakan akun di perangkat publik atau bersama, selalu log out dan hapus riwayat browser. Jangan simpan password di browser yang tidak aman.

## **TINGKATKAN LITERASI DIGITAL & EDUKASI ORANG SEKITAR**

Ikuti pelatihan keamanan digital jika ada. Edukasi keluarga atau teman, terutama yang awam teknologi, tentang modus phishing yang sering terjadi.



# INGAT!

**JANGAN LUPA MELAKUKAN PELAPORAN  
TERHADAP PIHAK BERWENANG JIKA  
MENDAPATI KEJADIAN PHISING INI!**

- Bank atau layanan terkait
- Polisi siber (Patroli Siber Bareskrim Polri)
- Lembaga pelapor phishing seperti IDADIX atau APWG

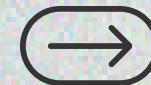






# KALAU TERLANJUR KENA GIMANA?

Terlanjur jadi korban phishing? Jangan panik, tetap tenang dan kamu tidak sendirian. Yang penting sekarang adalah bertindak cepat dan tepat untuk meminimalkan kerugian



# YANG HARUS DILAKUIN!

## PUTUSKAN AKSES PELAKU:

Segera tutup halaman,  
putuskan koneksi internet,  
atau tutup aplikasi yang  
terbuka

## AMANKAN AKUN YANG TERDAMPAK

mengganti password akun,  
mengaktifkan autentikasi dua  
faktor

## PERIKSA AKTIFITAS AKUN DAN TRANSAKSI TERBARU

cek Riwayat login dan aktivitas aneh  
di email, akun medsos, maupun e-  
wallet. Logout dari semua  
perangkat yang tidak dikenal

## MELAPORKAN KE LEMBAGA RESMI

seperti ke customer service akun terdampak, polisi siber (<https://patrolisiber.id/>),  
IDADX (Indonesia Domain Abuse Data Exchange)

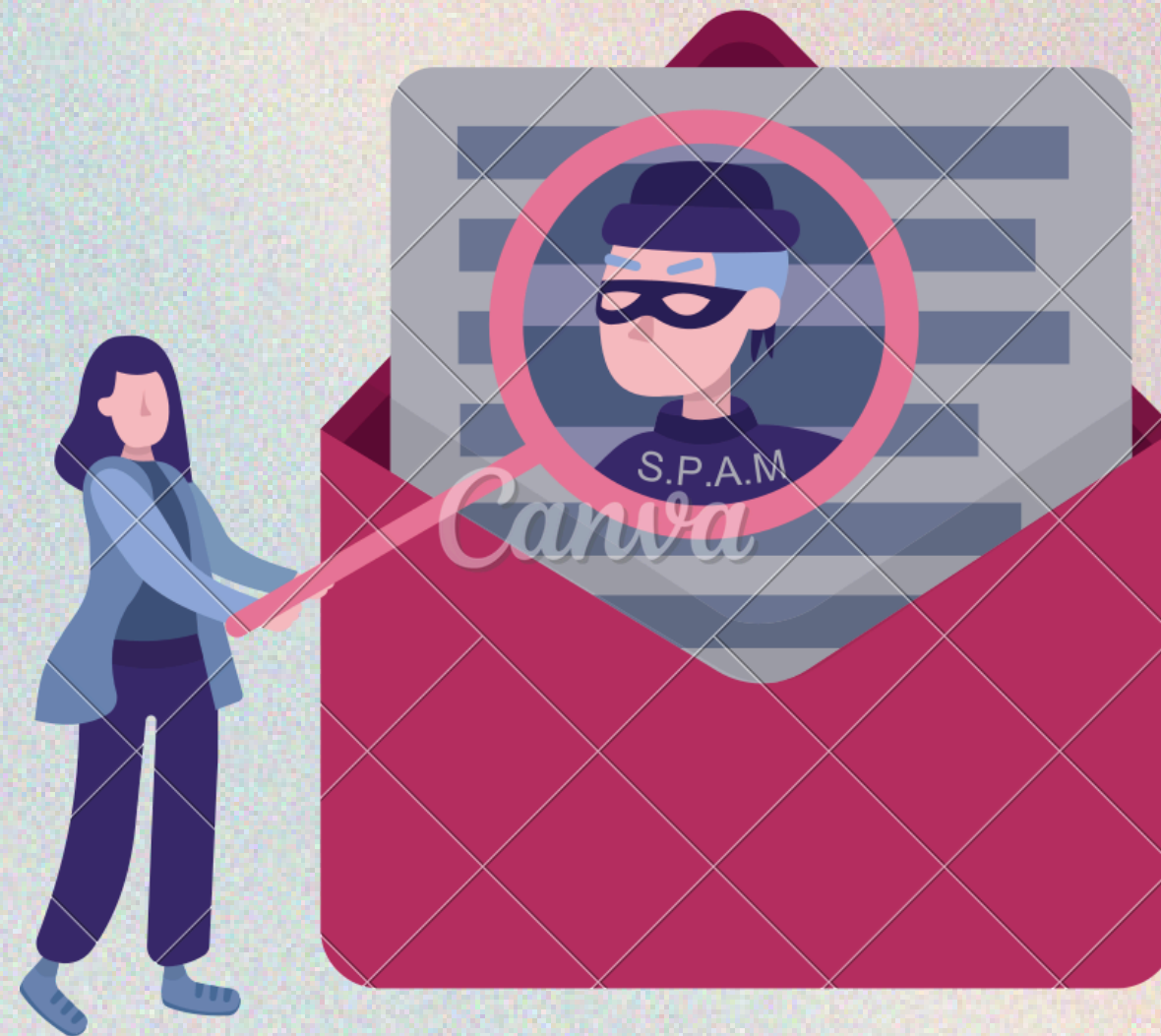






Literasi Media dan Informasi

# POST TEST ANTI-PHISNG





Literasi Media dan Informasi

**SETELAH MENJADI KORBAN PHISHING,  
CUKUP GANTI PASSWORD SAJA TANPA  
PERLU MELAKUKAN HAL LAIN**

**BENAR/SALAH?**





(+62)821-2588-0368  
Rover Clauridho



link web disini

# THANK YOU!

Semakin kita sadar akan bahaya phishing, semakin kecil kemungkinan kita jadi korban. Jangan mudah percaya, selalu cek ulang, dan lindungi informasi pribadimu. Karena keamanan digital dimulai dari diri sendiri