RISIKO PENIPUAN DAN SIBER

PANDUAN KEWASPADAAN DALAM BERBISNIS

Sudahkah Anda mengambil langkah untuk melindungi bisnis Anda?

BNP PARIBAS CASH MANAGEMENT

2025

BNP PARIBAS

The bank for a changing world

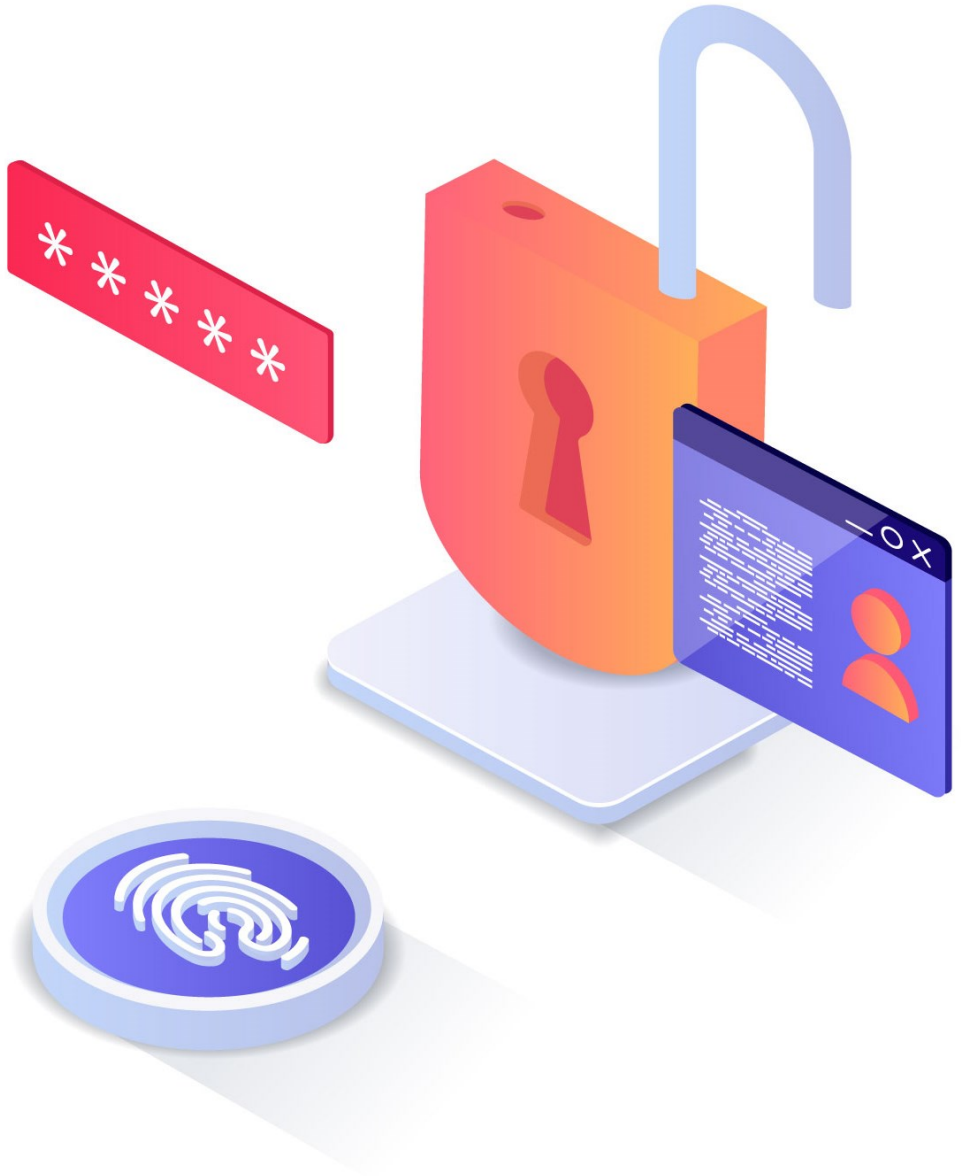
01 PENDAHULUAN
Buat karyawan Anda sadar tentang bahayanya!

02 IKHTISAR SKEMA PENIPUAN
Penipuan CEO palsu, penipuan pemasok palsu...

03 TEKNIK-TEKNIKNYA
Pencurian informasi dan rekayasa sosial, pemalsuan...

04 RISIKO-RISIKO SIBER
Phishing dan *spear phishing*, *malware*, *ransomware*...

05 KESIMPULAN
Kembangkan refleks yang tajam, jika terjadi transfer penipuan



BUAT KARYAWAN ANDA SADAR TENTANG BAHAYANYA!

Untuk melindungi perusahaan Anda dari kejahatan penipuan, tidak cukup hanya memiliki prosedur, alat dan kontrol.

Sangat penting untuk senantiasa menjaga karyawan Anda terinformasi dan terlatih, sehingga mereka dapat mendeteksi dan melawan upaya penipuan dan serangan siber. Di hampir semua kasus, **pelaku penipuan memanfaatkan kelemahan manusia**.

LAKUKAN:

- **Selanggarakan pelatihan rutin.** Jangan hanya mengandalkan pengiriman surel
- **Memastikan bahwa karyawan sementara dan karyawan dengan kontrak jangka waktu tertentu** mendapatkan orientasi awal tentang penipuan karena mereka adalah target yang ideal
- **Melatih karyawan bagian akuntansi dan perbendaharaan untuk meningkatkan kewaspadaan di antara semua karyawan** yang rentan tertipu untuk memberikan informasi kepada penipu (asisten...) atau secara tidak sengaja memasang malware di jaringan
- **Melatih kembali karyawan** paling sedikit satu kali dalam satu tahun. Ancaman terus berkembang dan karyawan Anda harus tetap waspada
- Selain **pelatihan, berikan instruksi tertulis yang jelas** kepada karyawan Anda (Kebijakan dan prosedur)

Dokumen ini berisi saran yang baik dan pedoman khusus yang dapat Anda adaptasikan ke bisnis Anda dan sampaikan kepada karyawan Anda.

IKHTISAR SKEMA PENIPUAN

PENIPUAN CEO PALSU

CONTOH

Anda menerima **surel** atau **pesan WhatsApp** atau **panggilan** dari pejabat eksekutif palsu yang memerintahkan Anda untuk melakukan pembayaran yang mendesak:

"Kita sedang melakukan pekerjaan keuangan yang harus dijaga kerahasiaannya. Saya memilih Anda karena kebijaksanaan dan kerja keras Anda. Firma hukum kita akan menghubungi Anda untuk memberikan rinciannya."

TANDA-TANDA PERINGATAN

- **Surel** tentang akuisisi suatu perusahaan, audit pajak...
- **Permintaan tak terduga dari pengacara**, pejabat eksekutif, anggota dewan...
- **Urgensi** dari situasi (akuisisi, pemeriksaan pajak, dll.)
- **Kerahasiaan** (*rahasia & sangat rahasia*) ("terutama untuk tidak membicarakannya; ini nomor telepon untuk mengenkripsi percakapan kita...")
- **Sanjungan** ("Saya diberitahu bahwa saya dapat mengandalkan Anda")
- **Intimidasi** atau pelecehan ("Tolong dengarkan saya! Hal ini mendesak!")

LINDUNGI DIRI ANDA

- **Waspada**, Manajemen tidak akan meminta Anda untuk melakukan pembayaran yang mendesak yang tidak mengikuti prosedur normal
- **Beri tahu penyelia Anda**. Orang yang bermaksud baik tidak akan meminta Anda untuk menyembunyikan informasi dari penyelia Anda
- **Patuhi pemisahan tugas**
  - Apabila Anda diperbolehkan untuk melakukan (atau mengatur satu kali) pembayaran besar sendiri, Anda berisiko; **otorisasi ganda** setidaknya harus diwajibkan
  - Hindari perintah dan validasi transfer melalui faks; mudah bagi penipu untuk mendapatkan contoh tanda tangan
  - Kata sandi dan proses masuk bersifat pribadi: Jangan pernah berikan kata sandi dan proses masuk kepada kolega; laporkan mereka apabila mereka mencoba memberikan milik mereka kepada Anda
- **Periksa dengan akal sehat:**
  - **Cek alamat surel**: penipu sering menggunakan alamat serupa (misal: john.smith@sale-team.com dan bukan john.smith@sales-team.com). (Lihat halaman 7)
  - **Cek identitas kontak Anda** dengan menghubungi mereka kembali menggunakan rincian yang diketahui dan terverifikasi, bukan yang diberikan oleh pengirim

DAN INGAT

- Penipu menggunakan platform telepon panggilan melalui internet (VoIP) yang **seolah-olah merupakan panggilan telepon lokal** di sebagian besar negara; mereka menggunakan teknik **pemalsuan nomor** (*caller ID spoofing)* untuk menyamarkan nomor telepon; mereka juga menggunakan panggilan atau pesan **WhatssApp**
- Penipu sering kali mengetahui banyak hal tentang bisnis Anda dan dapat meniru suara orang ("*deepfake*")
- Apabila penipuan gagal, penipu kemudian mungkin menghubungi CEO dengan berpura-pura sebagai petugas polisi atau bank

Kami mencatat adanya peningkatan peretasan alamat surel, jadi tetaplah waspada meskipun alamat surel tersebut sah

PENIPUAN CEO PALSU

Tanda-tanda yang seharusnya mengingatkan kita pada sesuatu!

- *Spoofing* surel
- Kegawatdaruratan / Menjelang hari libur...
- Konteks khusus
- Kerahasiaan
- Sanjungan
- Keterlibatan pihak ketiga (firma hukum...)

RE: MENDESAK – Untuk diproses pada kesempatan pertama !

JS

john.smith@qwerty-analysis.com <john.smith@presidency.com> Monday June 17 at 3:44 PM

À : kate@qwerty-analysis.com

Kate,

Selama beberapa bulan terakhir, kita telah bekerja sama, berkoordinasi, dan di bawah pengawasan OJK, untuk mengakuisisi sebuah perusahaan Tiongkok. Pengambilalihan ini harus tetap dirahasiakan, orang lain tidak ada yang perlu mengetahuinya untuk saat ini.

Pandemi COVID-19 tampaknya menguntungkan kita karena tawaran kita diterima lebih cepat dari perkiraan. Pengumuman publik mengenai pengambilalihan ini akan dilakukan pada hari Jumat, 4 Juli 2020 di kantor kita yang dihadiri oleh seluruh jajaran direksi.

Saya memilih Anda karena kebijaksanaan dan kinerja Anda yang luar biasa di perusahaan. Mohon segera hubungi firma hukum kita (robert.johns@kpmg-lawyer.com). Beliau akan segera memberikan rincian transfer bank.

Tolong kirimi saya saldo rekening.

Hal ini sangat sensitif, jadi mohon hanya berkomunikasi dengan saya melalui surel ini (john.smith@presidency.com), agar kita tidak melanggar peraturan OJK.

John Smith

PENIPUAN PEMASOK PALSU (DAN TUAN TANAH, ANJAK PIUTANG PALSU…)

CONTOH

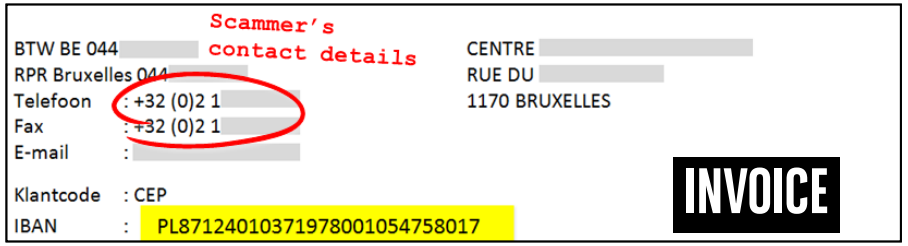
Pemasok palsu memberi tahu Anda (melalui surel, surat, telepon) bahwa rekening banknya berubah, dan semua faktur harus dibayarkan ke rekening baru:

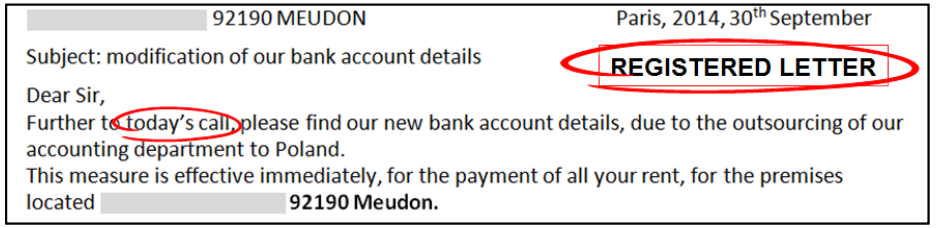
Informasi pembayaran

J **john@company.com** Today at 3:02 PM

À : kate@qwerty-analysis.com

Sehubungan dengan berita tentang pandemi virus Corona, kami mengganti bank dan mengirimkan pembayaran langsung ke pabrik kami untuk pembayaran, jadi harap beri tahu saya total pembayaran yang bisa dilakukan sehingga saya dapat meneruskan informasi pembayaran terbaru kami.





TANDA-TANDA PERINGATAN

- Permintaan apa pun **untuk mengubah rekening penerima** (melalui surat, surel, pada faktur, melalui telepon, dll.)
- Perubahan kontak pemasok terbaru (surel, nomor telepon…)

LINDUNGI DIRI ANDA

Ikuti prosedur dalam hal perubahan rincian rekening bank atau rincian kontak:

- **Cek identitas kontak** menggunakan **rincian kontak yang dapat diverifikasi** (dan bukan yang dikirimkan dalam faktur); jangan tunggu sampai Anda harus melakukan pembayaran
- **Berikan perhatian khusus kepada pemasok terbesar Anda**
- **Berhati-hatilah apabila rekening baru tersebut berdomisili di luar negeri**
  - Kode negara ISO: 2 huruf pertama dari IBAN dan huruf kelima dan keenam kode BIC
  - Siprus: CY17002001280000001200527600 - BIC: ABKLCY2N
  - Prancis: FR7630046001290029721519546 -BIC: ABCDFR1N
- Lengkapi prosedur Anda dengan Solusi Validasi Rekening, seperti yang diberikan oleh mitra BNP Paribas: Sis ID. (sis-id.com/en/). Mintalah demo kepada Relationship Manager Anda.
- **Tunjuk sedikit orang yang berwenang untuk mengubah rincian pemasok dan pastikan kontrol ganda atas perubahan**; latih orang-orang ini secara rutin dan tunjuk sebagai penanggung jawab

DAN INGAT

- Penipu menggunakan **surat tercatat**
- **Tuan tanah palsu** dan **anjak piutang palsu** merupakan variasi dari jenis penipuan ini:

"Untuk menyederhanakan struktur organisasi akuntansi dan fokus pada peningkatan produktivitas kami, penandatanganan kontrak anjak piutang dengan…"

- Sebelum menyerang, penipu umumnya **mencuri faktur asli** dari pemasok, menggunakan teknik peniruan atau peretasan
- **Hati-hati:** Penipu dapat menggunakan alamat surel yang mirip dengan pemasok Anda – **atau memang sama persis**; kemudian membajak surel Anda (Lihat halaman 7)

Kami mencatat peningkatan peretasan alamat surel, jadi tetap waspada meskipun alamat surel tersebut sah.

PENIPUAN TEKNISI PALSU

CONTOH

Penipu berpura-pura sebagai teknisi bank menghubungi Anda, mengatakan bahwa terdapat malfungsi atau perlunya menjalankan beberapa tes.

Dengan uraian menggunakan kontrol psikologis yang rumit yang membuat Anda sangat percaya, penipu berhasil mengambil kode akses dan validasi Anda ke situs perbankan daring.

Dengan menghubungkan ke perangkat Anda dari jarak jauh, penipu bebas mengeluarkan dan memvalidasi pembayaran untuk keuntungannya.

Dengan pendekatan yang berbeda, berdasarkan teknik serupa, pada dasarnya penipu akan mengambil alih kontrol komputer Anda, dengan cara membuat Anda menerima kendali atas PC Anda secara langsung darinya.

TANDA-TANDA PERINGATAN

- **Seseorang menawarkan untuk membantu Anda dengan sarana pembayaran Anda** ketika Anda tidak meminta bantuan tersebut secara langsung
- **Pertanyaan mengenai sarana atau prosedur pembayaran Anda**
- **Tautan yang Anda tidak kenal** (contoh URL pendek seperti: www.id5.com/bnp, www.tin.com/sepa08, www.tinyurl.com/migr, dll.)
- **Permintaan untuk mengambil kendali PC Anda dari jarak jauh**
- **Permintaan untuk melakukan uji coba transfer**
- **Pendekatan yang mengancam**, berpura-pura, contohnya rekening Anda mungkin diblokir atau pembayaran Anda diproses dua kali kecuali Anda memberitahukan kode Anda kepada penelepon. Ingat bahwa staf BNPP tidak pernah meminta Anda untuk memberikan kode Anda melalui telepon atau surel.

Penipu mungkin menghubungi korbannya setelah melakukan penipuan dan mengajukan pertanyaan dengan berpura-pura membantu korbannya mendapatkan uangnya kembali. Pada kenyataannya, mereka mengumpulkan informasi untuk meningkatkan teknik penpuan mereka. Apabila Anda pernah menjadi korban penipuan dan penipu tersebut menghubungi Anda kembali, tutup teleponnya segera.

LINDUNGI DIRI ANDA

- **Jangan percaya ID penelepon**: penipu mungkin menyamar sebagai nomor telepon Relationship Manager Anda (*spoofing* telepon)
- **Hubungi Relationship Manager Anda** dengan menggunakan rincian yang diketahui untuk meverifikasi identitas dari siapapun yang mengklaim sebagai karyawan BNP Paribas (atau karyawan pemasok perangkat lunak)
- **Tolak untuk mengizinkan PC Anda dikendalikan dari jarak jauh oleh siapa pun yang tidak dapat Anda verifikasi**, jangan pergi ke alamat Internet, jangan klik tautan/unduhan
- **Jangan pernah melakukan uji coba atas permintaan teknisi**: jangan mengkredit rekening pihak ketiga, jangan mengkonfirmasi suatu transaksi atau transfer; meskipun atas inisiatif Anda sendiri, jangan pernah melakukan uji coba dengan lebih dari €1 (*penny test*)
- **Jangan pernah berikan kode apapun kepada siapapun** (misalnya nomor yang dihasilkan pembaca nirkabel Anda, kata sandi, kode PIN, dll.)
- **Lindungi jaringan komputer dan PC Anda** dari peretasan dan perangkat lunak berbahaya, dengan memastikan pembaruan/*patch* rutin

DAN INGAT

- **Teknisi BNP Paribas tidak akan pernah menghubungi Anda** kecuali Anda meminta bantuan secara langsung
- Penipu juga dapat mengklaim sebagai **pemasok perangkat lunak perbankan Anda**
- **Penipu mengetahui sistem perbankan dengan sangat baik**; mereka bahkan mungkin menyadari isu-isu terkini; bahkan nama Relationship Manager Anda
- Untuk menipu Anda, penipu mungkin melakukan **beberapa panggilan awal untuk membangun kepercayaan**, tanpa menipu Anda pada saat pertama kali
- Apabila Anda dilengkapi dengan pembaca nirkabel, penipu mungkin berkata: "Jangan beritahu saya kode PIN Anda, Saya tidak seharusnya mengetahuinya; **cukup berikan kode yang ditampilkan pada pembaca nirkabel**"
- **Skema baru penipuan jenis ini melibatkan dengan cara menghubungi Anda untuk memperbarui alat identifikasi BNP Paribas Anda. Waspadalah!t**

PENIPUAN KARYAWAN / GAJI PALSU

CONTOH

Skema ini mirip dengan penipuan pemasok:

- **Karyawan palsu memberi tahu Anda (melalui surel, surat, telepon) bahwa rekening bank mereka telah berubah dan gaji mereka harus dibayarkan ke rekening baru tersebut.**
- **Perusahaan Anda akhirnya membayar ke rekening penipu.**

RE: Rekening Baru

JS ⊗ **john.smith@gmail.com** 26/07 - 12:02

To : kate@qwerty-analysis.com

Halo Kate,

Saya menghubungi Anda dengan alamat surel pribadi saya karena saya tidak bisa lagi terhubung ke alamat kantor saya sejak kemarin. Saya sudah menyampaikannya kepada tim dukungan TI, tetapi mereka masih menunggu balasannya. Saya lebih suka menghubungi Anda segera.

Saya baru saja berganti bank dan ingin mentransfer gaji saya berikutnya dengan rekening terlampir.

Salam,
John Smith

TANDA-TANDA PERINGATAN

- Setiap permintaan **perubahan rekening penerima** (melalui surat, surel, pada faktur, melalui telepon, dll.)
- **Perubahan kontak** karyawan yang baru-baru ini (surel, nomor telepon,...)
- Berhati-hatilah terutama jika rekening tersebut berada di **negara asing** atau di **bank non-tier-1** (khususnya bank-bank digital)

LINDUNGI DIRI ANDA

Ikuti prosedur dalam hal terjadi perubahan rincian rekening bank atau rincian kontak:

- **Cek identitas** kontak Anda menggunakan **rincian kontak yang dapat diverifikasi** (dan bukan yang dikirimkan dalam surel); jangan menunggu sampai Anda harus melakukan pembayaran
- **Berhati-hatilah jika rekening baru tersebut berada di luar negeri**
  - Kode negara ISO: 2 huruf pertama IBAN dan huruf kelima dan keenam kode BIC
  - Siprus: CY17002001280000001200527600 - BIC: ABKLCY2N
  - Prancis: FR7630046001290029721519546 -BIC: ABCDFR1N
- Lengkapi prosedur Anda dengan **Solusi Validasi Rekening**, seperti yang diberikan oleh mitra **BNP Paribas: Sis ID**. (sis-id.com/en/). Mintalah demo kepada Relationship Manager Anda.
- **Tunjuk sedikit orang yang berwenang untuk mengubah rincian pemasok dan pastikan kontrol ganda atas perubahan**; latih orang-orang ini secara rutin dan tunjuk sebagai penanggung jawab

DAN INGAT

- Penipu menggunakan **surat terdaftar**
- Penipu **sering kali mengetahui perusahaan dengan sangat baik** dan dapat menggunakan informasi yang dikumpulkan di internet untuk menyamar sebagai karyawan Anda.
- **Peringatan!** Hingga saat ini, jenis penipuan ini umumnya dilakukan melalui surel dan semakin canggih dan berbahaya. Penipu tidak ragu untuk melakukan panggilan telepon, meniru suara, dll.
- **Cek alamat surel!** Penipu terkadang menggunakan alamat yang mirip (contoh jean.dupont@sale-team.com dan bukan jean.dupont@sales-team.com), **tetapi hati-hati: penipu juga bisa menulis dari kotak surat sah karyawan yang berhasil mereka retas** (kasus ini semakin sering terjadi)

PENIPUAN *PHISING* – MELALUI SUREL ATAU PESAN TEKS

CONTOH

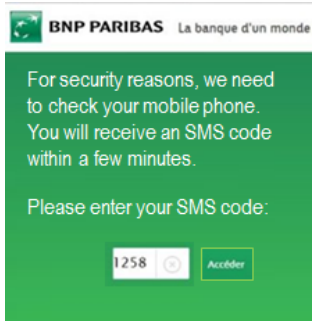
Anda menerima surel yang tampaknya berasal dari bank Anda. Apabila Anda mengklik tautan, halaman bank palsu terbuka dan meminta informasi (kata sandi, nomor kartu kredit, dll.). Penipu juga dapat mencuri kode SMS yang dikirimkan oleh bank Anda untuk memvalidasi suatu akun atau pembelian menggunakan kartu

Anda memiliki pesan baru

J **john@bnpparibas.com** Today at 9:02 AM

To : kate@qwerty-analysis.com

Nasabah yang terhormat,
Anda memiliki 2 pesan baru. Periksa kotak masuk Anda dengan mengklik tautan dibawah
Your mailbox



Phising sangat umum, dan dapat mempengaruhi **telepon perusahaan Anda, pemasok listrik atau gas**, **administrasi**, **penyedia surel** Anda (Gmail, Hotmail...), **media sosial**, dan banyak lagi.

Info: kami menerima permintaan dari kartu SIM baru untuk kontrak seluler Anda. Apabila bukan Anda yang melakukan permintaan ini, harap segera hubungi Layanan Bantuan di 12345

Penipu juga dapat menyadap kode yang dikirim melalui SMS oleh bank Anda dengan meminta kartu SIM baru yang dikirim oleh operator telepon Anda. Hal ini dikenal sebagai SIM *swapping*.

TANDA-TANDA PERINGATAN

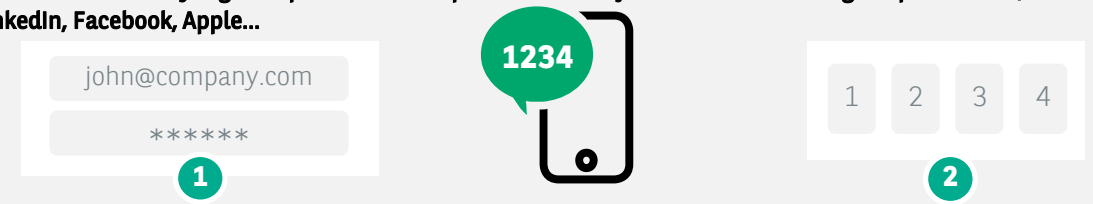
- **Surel yang seolah berasal dari lembaga** memiliki hubungan Anda (LinkedIn, bank, pemasok, nasabah, otoritas pajak...), dengan tautan atau lampiran
- **Permintaan tidak terduga** yang tampaknya memiliki dasar logis (faktur...)
- **Pesan yang mengkhawatirkan atau menghasut** yang mendesak Anda untuk membuka atau mengklik file
- **Ketidaksesuaian** dalam surel (ejaan...)

LINDUNGI DIRI ANDA

Kembangkan refleks yang tajam!

- Periksa dengan teliti **perhal** dan **isi surel** (ejaan, pesan yang mengkhawatirkan...), serta alamat surel pengirim, terutama *domain*
- Sebagai aturan umum, jangan buka lampiran dan **jangan klik tautan atau gambar yang dapat diklik yang diberikan di dalam surel yang Anda terima**
- Untuk mengakses sarana perbankan atau aplikasi media sosial Anda, selalu gunakan aplikasi asli atau gunakan Favorit atau mengingat alamat yang biasa ke peramban Anda; cek adanya **https://** dan **ikon gembok**
- Apabila Anda tidak sengaja mengklik tautan dalam surel, jangan masuk di situs web tersebut: **jangan masukkan kata sandi, atau kode yang dikirimkan melalui SMS**
- Jangan membuka atau membalas surel yang mencurigakan; jangan menelepon nomor telepon yang diberikan dalam surel tersebut

Gunakan otentikasi yang kuat pada situs web perbankan. Aktifkan autentikasi 2 langkah pada Gmail, Hotmail, LinkedIn, Facebook, Apple...



Anda memasukkan rincian masuk seperti biasa ▶ Kami mengirimkan **kode verifikasi** pada perangkat Anda ▶ Anda memasukkan kode tersebut untuk memverifikasi identifas Anda

DAN INGAT

- Apabila Anda mengalami **masalah pada ponsel Anda** (kehilangan jaringan dalam jangka waktu lama, kartu SIM tidak valid), Anda mungkin menjadi korban **SIM *swapping***, hubungi operator telepon Anda
- *Spear phising* adalah serangan *phising* yang ditujukan pada individu atau perusahaan tertentu untuk mencuri data, memasang *malware*, dll; pengirimnya mungkin tampak seperti seseorang yang Anda kenal
- **Cek tautan dengan mengarahkan kursor ke URL**, alamat penerusan akan ditampilkan di bagian bawah navigator Anda)

PENIPUAN *PHISING* – MELALUI PENCARIAN INTERNET/SITUS PALSU

CONTOH

Anda mencari situs perbankan Anda pada mesin pencari Anda biasanya dengan memasukkan kata kunci Anda biasanya. Apabila Anda tidak memperhatikannya, Anda mengklik tautan yang salah: **halaman internet palsu** dari bank terbuka dan meminta informasi (kata sandi, nomor kartu bank, dll.). Terkadang penipu juga dapat menarik data yang dikirimkan kepada Anda melalui SMS atau surel dari bank Anda untuk memvalidasi perangkat, rekening atau pembelian menggunakan kartu.

Ini adalah teknik *phising* tanpa penargetan khusus, tetapi dapat mempengaruhi semua orang yang penggunanya mengakses situs melalui mesin pencari.

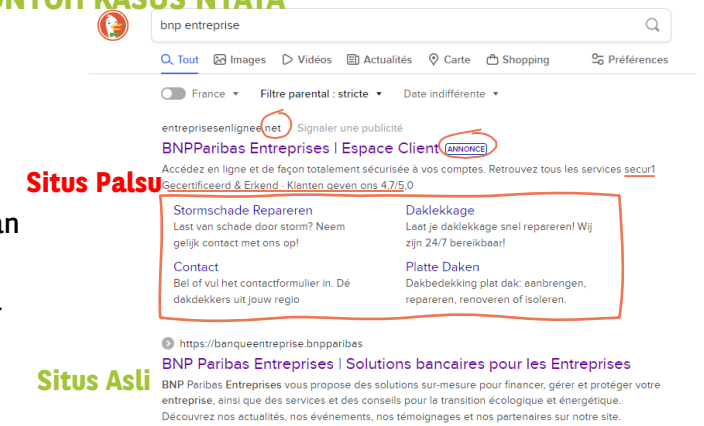
Penipu membuat **situs web yang secara visual mirip dengan situs resmi** dari laman mana pun dan secara artifisial menaikkan peringkatnya dalam pencarian melalui iklan bersponsor, menggunakan teknik referensi yang canggih, sehingga situs palsu muncul pertama kali dalam pencarian.

TANDA-TANDA PERINGATAN – CONTOH KASUS NYATA

- Tautan bersponsor
- Ekstensi yang tidak lazim
- Ketidakkonsistenan bahasa

<u>+ di situs:</u>

- Ketidaksesuaian apapun (kesalahaan eja, logo lama ...).
- Isi yang tidak sesuai dan/atau lama
- Tidak ada akses yang diberikan meskipun ID login dan kata sandi sudah benar



LINDUNGI DIRI ANDA

- **Jangan menggunakan mesin pencari untuk menemukan situs bank elektronik Anda:**
  - Tandai di favorit
  - Atau masukkan alamat lengkap pada bilah peramban Anda
- **Namun, apabila Anda harus menggunakan mesin pencari, BERHATI-HATILAH:**
  - **Masukkan alamat lengkap**, bukan kata kunci standar
  - **Jangan klik tautan bersponsor**
  - **Baca alamat situs dengan teliti sebelum mengklik** untuk mendeteksi anomali (huruf hilang atau ditambahkan, tanda hubung tambahan, ekstensi tidak biasa, bahasa tidak sesuai
  - **Cek bahwa deskripsi situs sesuai dan ditulis dalam bahasa yang tepat**
  - **Pastikan tidak ada fitur yang tidak biasa**: karakter tertentu, bahasa yang tidak sesuai untuk situs yang dikunjungi...
- **Jangan berbagi sarana akses Anda**, bahkan di antara rekan kerja
- **Gunakan otentikasi kuat yang ditawarkan oleh bank Anda**. Cek surel peringatan yang dikirimkan oleh bank Anda dan beritahukan segera apabila Anda menerimanya untuk tindakan yang tidak Anda lakukan.

DAN INGAT

- Tautan berikut adalah tautan resmi ke situs milik BNP Paribas :
  - Connexis Cash : https://connexis.bnpparibas.com/
  - MaBanqueEntreprise : https://mabanqueentreprise.bnpparibas/
  - MaBanque : https://mabanque.bnpparibas/
  - MaBanquePro : https://mabanquepro.bnpparibas/
  - MaBanquePrivée : https://mabanqueprivee.bnpparibas
- **Jangan beritahukan kode apa pun** kepada siapa pun
- Beberapa penipu meretas kode sekali pakai yang dikirimkan melalui SMS (teknik *SIM SWAPPING*). **Apabila Anda mengalami anomali dengan telepon seluler Anda (kehilangan jaringan untuk waktu yang lama) hubungi operator Anda.**

PENIPUAN CEK/BILYET GIRO (BG)

CONTOH

Mengirimkan cek/BG kemudian meminta pengembalian dana melalui transfer bank

Nasabah atau calon nasabah mengirimkan pembayaran berupa cek/BG kepada Anda, dengan jumlah yang jauh lebih tinggi daripada faktur. Dengan dalih terjadi kesalahan, ia meminta Anda untuk mencairkan cek/BG dan mengembalikan kelebihan yang diterima melalui transfer bank, dikurangi komisi untuk meminta maaf atas kendala tersebut.

Cek/BG ternyata palsu, tetapi transfer Anda nyata.

Varian: cek/BG-nya bisa saja berjumlah tepat dan nasabah palsu tersebut dapat langsung meminta pengembalian dana melalui transfer dana, dengan mengklaim pembatalan.

*"Terlampir pembayaran tagihan sewa ruang seminar yang dijadwalkan 2 bulan mendatang." Jumlahnya **dua kali lipat** dari yang diharapkan* ▶ *"Mohon maaf, saya salah memasukkan jumlah yang tercantum dengan penawaran lain. Bisakah Anda mentransfer kelebihannya? Mohon simpan sisa 10% di rekening Anda sebagai permintaan maaf atas ketidaknyamanan ini"*

Ada jenis penipuan lain dengan cek/BG

- Digunakan oleh penjahat untuk mengambil **cek/BG yang hilang atau dicuri**.
- **Pemalsuan cek oleh penjahat**. Proses ini dilakukan dengan cara menipu, mengubah jumlah atau penerima cek/BG yang sah, misalnya dengan mencurinya dari kotak surat penerima

TANDA-TANDA PERINGATAN

- **Seseorang yang berdomisili di luar negeri**, menghubungi Anda melalui surel (ditulis dalam bahasa Inggris atau bahasa Prancis yang sangat mendekati) dan mengatakan bahwa ia tertarik untuk memperoleh barang atau jasa.
- Pembeli kemudian mengirimkan **cek/BG kepada Anda dengan jumlah yang jauh lebih tinggi daripada yang disepakati sebelumnya dan menemukan alasan untuk membenarkan perbedaan tersebut**.
- Ia meminta Anda untuk **mengembalikan sebagian kelebihan tersebut kepadanya dan Anda akan menerima kompensasi** yang besar atas biaya dan ketidaknyamanan Anda.

LINDUNGI DIRI ANDA

- **Apabila Anda menerima pembayaran dengan cek/BG dan menerima cek/BG untuk jumlah yang lebih besar daripada penjualan, kami sarankan Anda untuk tidak mencairkannya** sebelum memastikannya.
- **Jangan pernah mengganti uang nasabah melalui transfer bank apabila ia membayar dengan cek/BG sebelum Anda telah memastikan dengan bank Anda bahwa cek/BG tersebut telah dicairkan** sebagaimana mestinya (fakta bahwa jumlah yang muncul pada rekening Anda tidak berarti bahwa bank telah memeriksa apakah cek/BG telah dibayar atau belum).
- **Sebisa mungkin pilih pembayaran elektronik daripada cek/BG**, terutama di luar negeri (waktu pemrosesan lebih lama dan rumit, dll.).
- **Buku cek/BG harus disimpan di tempat yang aman**. Ada banyak peluang terjadinya pencurian, terutama saat mengirimkan buku cek/BG.
- **Dalam hal penipuan, laporkan fakta-faktanya kepada polisi**. Simpan semua dokumen milik Anda (surel yang dipertukarkan dengan penipu, cek/BG dll.) untuk memudahkan penyelidikan.

DAN INGAT

- **Peraturan di Indonesia tidak menetapkan jumlah maksimum untuk cek/BG**, tetapi transaksi tertentu seperti pembelian mobil bekas antara individu, cek/BG bank tetap dimungkinkan.
- Dalam hal terdapat kesalahan dalam penyusunan cek/BG Anda dengan **perbedaan antara jumlah dalam angka dan dalam huruf, hanya jumlah dalam huruf yang dapat diperhitungkan saat pencairan!** (KUHD Pasal 186).
- **Di Indonesia, Cek yang diterbitkan berlaku selama 70 hari + 6 bulan sejak tanggal penarikan (termasuk masa daluwarsa); Tenggang waktu pengunjukan BG adalah 70 hari sejak tanggal penarikan**.

⚠ ***Biasanya, cek dikreditkan paling lambat satu hari kerja setelah didaftarkan atau tergatung wilayah kliring dilakukan***

PENIPUAN PEMBAYARAN (KARTU KORPORAT)

CONTOH

Penjaht mencuri rincian bank (nomor kartu, kode kartu kredit, kode SMS) untuk melakukan pembayaran atas nama pemegang yang sah, untuk kepentingannya sendiri.

"Halo, saya SMITH, teknisi BNPP, saya menghubungi Anda mengenai transaksi tidak biasa yang terdeteksi pada kartu pembayaran Anda.
Apakah Anda baru-baru ini melakukan pembayaran sebesar €936.5 kepada Primark"

Ada beberapa jenis penipuan kartu:

- **Penipuan setelah kehilangan atau pencurian kartu**: terutama setelah mengamati kode Anda, penjahat akan menggunakan tipu daya untuk mencuri kartu Anda.
- ***Fraud White Plastic Skimming***: ATM yang dirusak memungkinkan penipu untuk menyalin kartu Anda. Praktik ini khususnya dilakukan di negara-negara yang hanya menggunakan jalur CB
- Penipuan internet: pencurian data kartu
  - **SIM *SWAP***: Beberapa penipu meretas kode sekali pakai yang dikirimkan melalui SMS oleh bank Anda dengan meminta kartu SIM dikirimkan kepada mereka oleh operator telepon Anda.
  - **Peniruan pihak ketiga tepercaya: Penipu menghubungi nasabah dengan berpura-pura sebagai lembaga yang dikenal** (OJK, BI, dll.), departemen *fraud* BNP Paribas, atau entitas yang dapat dipercaya.

TANDA-TANDA PERINGATAN

- Selama panggilan berlangsung, **nasabah ditekan** karena menghadapi **keadaan darurat**, misalnya penipuan yang sedang berlangsung.
- Pihak lawan bicara meyakinkan nasabah dengan memintanya untuk membatalkan pembayaran yang telah dilakukan **melalui kode yang diterima melalui SMS**. Kode ini sebenarnya untuk memvalidasi pembayaran.

LINDUNGI DIRI ANDA

- **Jangan bergantung pada angka yang ditampilkan**, karena penipu dapat memalsukan nomor yang sah.
- Apabila ragu dengan pihak lawan bicara, **tutup telepon dan hubungi pihak biasanya** berdasarkan rincian kontak yang tepercaya.
- **BNP Paribas tidak akan pernah meminta untuk memvalidasi transaksi melalui telepon.**
- Dalam hal terdapat tindakan mencurigakan atau meragukan, **segera ubah kode koneksi, dan hubungi BNP Paribas** untuk menerapkan langkah-langkah keamanan yang tepat, misalnya memperbarui kartu.
- Senantiasa terinformasi dan komunikasikan kepada tim Anda:

ECB – Laporan fraud kartu di Wilayah Eropa: Laporan ketujuh mengenai kejahatan kartu (Bahasa Inggris)

UK Finance – Peringatan penipuan: Panggilan otomatis palsu yang mengklaim sebagai bank dan perusahaan kartu (Bahasa Inggris)

DAN INGAT

- **Dalam hal terdapat penipuan pada kartu Perusahaan, Pengadaan, Virtual, Perjalanan atau Pembelian BNP Paribas Anda:**
- **1. Segera blokir kartu:**
  - melalui telepon dengan menghubungi layanan pelanggan khusus atau pusat oposisi
  - secara daring di situs web yang didedikasikan untuk mengelola kartu
- **2. Segera ajukan sengketa transaksi penipuan**
  - Apabila Anda keberatan melalui telepon, narahubung Anda akan memandu Anda melalui proses ini. Apabila Anda keberatan melalui internet, formulir keberatan tersedia langsung secara daring. Anda dapat mengajukan sengketa dalam jangka waktu terbatas (Anda akan menemukan jangka waktu ini dalam Ketentuan Pengoperasian kartu Anda).

Diperkirakan saat ini sekitar 90% penipuan yang dialami nasabah kami terkait dengan teknik pencurian identitas oleh pihak ketiga tepercaya.

Kartu Kredit Korporat belum tersedia di BNP Paribas Indonesia

TEKNIK-TEKNIKNYA

PHISHING – SARANA UTAMA YANG DIGUNAKAN PENIPU

DEFINISI

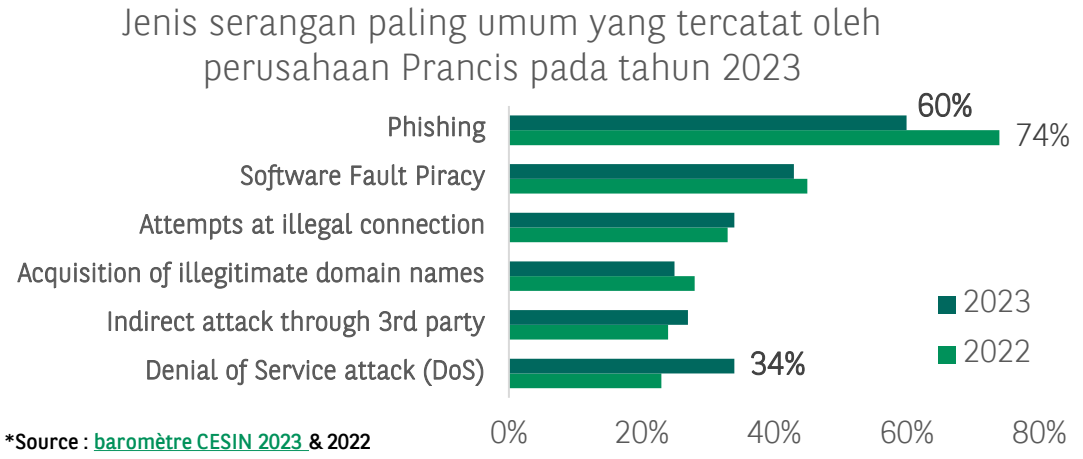
« Upaya untuk menipu seseorang agar memberikan informasi melalui internet atau surel yang memungkinkan orang lain untuk mengambil uang dari mereka, misalnya dengan mengambil uang dari rekening bank mereka »

Source: PHISHING | English meaning - Cambridge Dictionary/

Apabila Anda menerima surel dari pengirim yang menyebut dirinya sebagai badan resmi atau badan yang dikenal dan ingin mengakses data pribadi Anda di Internet, **Anda harus menolaknya**.

***Phising* sangat umum terjadi**, dan dapat melibatkan operator telepon Anda, pemasok listrik atau gas Anda, administrasi, surel online, media sosial, dll. Ini menyangkut alamat surel dan nomor telepon pribadi dan profesional.

Ini merupakan sarana utama serangan siber, karena ini adalah salah satu cara paling mudah untuk diatur.



*Source : baromètre CESIN 2023 & 2022

CONTOH :

- ***Phising* yang diterima melalui surel**
  - Cek dengan teliti perihal surat, isi dan alamat surel dari surat-surat yang Anda terima.
  - Dengan menggunakan konteks yang kredibel, penipu akan memainkan kartu peluang atau ancaman untuk mengundang Anda untuk mengklik tautan dan mengirimkan informasi Anda.

Anda memiliki pesan baru

A **primevideo@nanbV1.com** Today at 9:02 AM

To : Tom.STROA@Lycos.com

Hello Tom,
Hari terakhir untuk uji coba penawaran "Prime Video" kami. Perpanjangan otomatis langganan Anda telah berhasil. **Faktur sebesar EUR 380 (TTC)** akan dikirimkan ke alamat Anda. Anda memiliki waktu 5 hari untuk membatalkan pesanan dengan mengklik tombol di bawah ini:

Cancellation

- ***Phising* melalui SMS/pesan teks**
  - Cek nomor dan isi dengan teliti. Jangan klik tautan apa pun. Sambungkan langsung dengan situs apabila ragu-ragu.
  - Kewaspadaan mutlak dalam semua kasus yang diketahui di bawah ini:

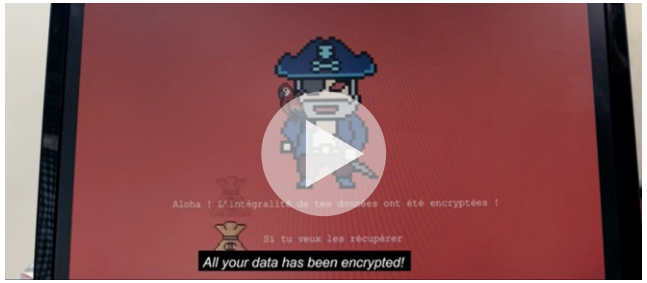
- << Halo Ayah, ini nomor telepon baruku. Bisa whatsapp ke alamat ini: XXX ? >>
- << Selamat pagi, Ini dari kurir pengiriman. Paket Bapak/Ibu tidak bisa dikirimkan. Mohon pesan slot waktu baru ke alamat ini XXX >>
- << DHL: Karena kecelakaan, pengiriman Anda tidak bisa dilakukan. Tindakan diperlukan dari Anda di XXX. >>
- << Netflix: Langganan Anda telah diblokir. Silakan perbarui informasi Anda di alamat ini XXX >>

PENCURIAN INFORMASI DAN REKAYASA SOSIAL

CONTOH

Anda menerima surel, surat atau panggilan telepon dari seseorang yang meminta informasi (faktur, biaya sewa, rincian kontak...):

"Sebagai bagian dari audit deklarasi ppn Anda, mohon berikan rincian dua pemasok tetap terbesar Anda, laporan rekening, dan duplikat faktur untuk masing-masing pemasok tersebut."



VIDEO LAINNYA
(Bahasa Inggris)
Dave the medium

Source : https://vimeo.com/962159764/61deee4306

TANDA-TANDA PERINGATAN

- **Seseorang yang tidak dikenal** menghubungi Anda untuk alasan apa pun dan meminta informasi yang tampaknya sepele
- **Permintaan apa pun mengenai faktur Anda, klien Anda, kontrak sewa Anda, dll** dari seseorang yang mengaku sebagai klien, auditor, otoritas pajak Anda...

LINDUNGI DIRI ANDA

Verifikasi identitas siapa pun yang meminta informasi

- Jangan berikan informasi **kepada orang yang tidak Anda kenal** (*head-hunter,* lembaga survei, kolega tidak dikenal, dll.)
- Bersikaplah sangat curiga kepada orang yang meminta informasi tentang **faktur**, **klien**, **pemasok**, **pembayaran**, **sewa**, prosedur dan **alat pembayaran** Anda
- Selalu verifikasi identitas kontak Anda dengan menggunakan rincian kontak yang diketahui (dan bukan yang diberikan oleh koresponden)

Batasi jumlah informasi yang tersedia secara publik

- Batasi jumlah informasi yang tersedia **di Internet** (media sosial, blog, situs web)
- Jangan mengedarkan dokumen yang berpotensi sensitif (templat surat, **tanda tangan**)
- Jika memungkinkan, gunakan **tanda tangan yang berbeda** untuk perintah bank dibandingkan dengan tanda tangan yang terdapat pada dokumen yang tersedia untuk umum
- Bersikaplah **bijaksana di luar perusahaan** mengenai peran Anda (persiapan pembayaran, wewenang penandatanganan...)

Jika memungkinkan, enkripsiKAN informasi sensitif dan gunakan TLS untuk komunikasi surel eksternal

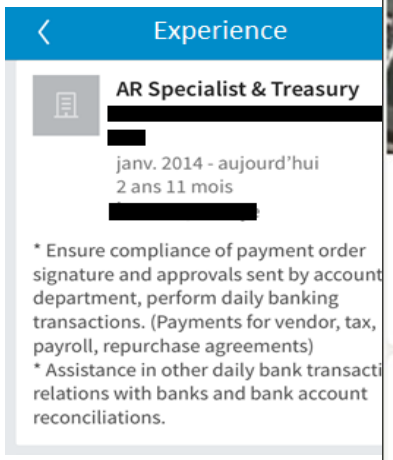
DAN INGAT

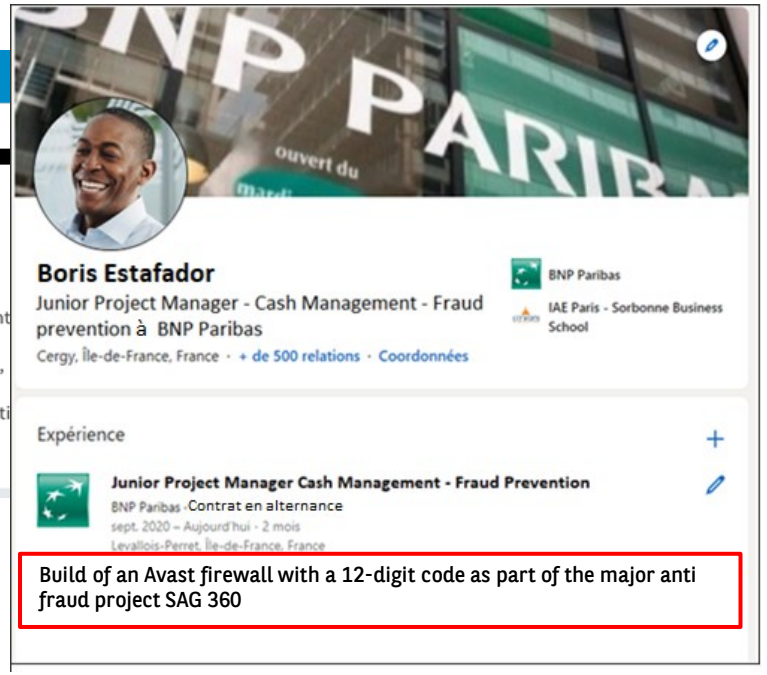
- **Segala jenis informasi, tidak peduli seberapa sepele** dapat dimanfaatkan oleh penipu (tanggal libur, alamat surel, nama anak, dll.)
- "**Internet jarang lupa**": Setelah informasi dipublikasikan di Internet, sulit untuk menghapusnya.

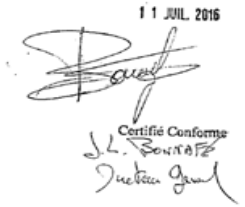
PENCURIAN INFORMASI DAN REKAYASA SOSIAL

Teknik pengumpulan data yang digunakan oleh peretas

Pengumpulan data di media sosial, daftar bisnis, pesan di luar kantor...







Companies House

KOMPASS

Panggilan surveyor, auditor, agen perjalanan, head-hunter, administrasi publik, pusat panggilan palsu...

Panggilan voice over IP yang mensimulasikan nomor lokal, penyamaran ID pemanggil (*spoofing*), perangkat lunak pengubah suara, pengalihan saluran telepon...

WhatsApp

voxbone
Local numbers, Global network

PENYAMARAN ALAMAT SUREL *(SPOOFING)*

CONTOH

Penjahat sering kali menggunakan alamat surel yang mirip dengan alamat surel korban yang identitasnya mereka ambil: ini disebut *spoofing* surel, dan berikut beberapa contohnya:

- Pemalsuan alias: bill.gates@microsoft.com <fraudster@gmail.com>
- Penggunaan sub-domain: bill.gates@microsoft.presidency.com
- Alamat "Dari" yang asli, alamat "Balas-Ke" yang palsu:
- Dari: bill.gates@legit-company.com
- Balas ke: bill.gates@legit-company.presidency.com
- Nama merk dengan tanda hubung ('-'): bill.gates@microsoft-corp.com
- Homograf nama merek: menggantikan 'O' dengan '0', 'l' dengan kapital 'i', 'I' atau 'L' dengan '1' ...: bill.gates@1egit-company.com
- Nama merek yang salah eja: bill.gates@nnicrosoft.com
- Penggunaan domain yang tidak umum: bill.gates@microsoft.top

Yang jarang terjadi, penipu memalsukan *header* surel, atau bahkan mengambil alih kontak masuk surel pengirim.

TANDA-TANDA PERINGATAN

- Sebagian besar peringatan berasal dari **perihal atau isi surel** itu sendiri (permintaan informasi, transfer mendesak, perubahan rekening...), atau dari pengirim yang tidak biasa atau tidak dikenal
- Sebagai aturan umum, perhatikan **alamat surel pengirim**, terutama apabila perihal atau isi surel mencurigakan
- Surel yang dikirim ke **kotak spam** Anda kemungkinan besar adalah surel palsu
- Tata bahasa yang buruk atau **kesalahan ejaan** adalah tanda-tanda yang jelas; jangan klik tautan atau membuka lampiran

LINDUNGI DIRI ANDA

Kewaspadaan saat menerima surel

- Dalam hal terdapat keraguan mengenai surek, jangan dibalas; hubungi koresponden Anda menggunakan rincian yang terverifikasi
- Pelajari cara memeriksa alamat surel dengan cermat, dalam hal terdapat permintaan yang mencurigakan atau sensitif, atau terdapat pengirim yang tidak biasa, untuk hal ini, pelajari untuk membaca header surel yang terperinci

BACA LEBIH LANJUT (Bahasa Inggis)
Petunjuk untuk membaca kepala surat elektronik lebih terperinci

Otentikasi surel surel dan penyaringan surel

- Departemen TI Anda dapat memantau atau memesan **nama domain** yang mirip dengan domain perusahaan Anda
- Mereka juga bisa **menyaring surel yang tidak diotentikasi** dengan protokol standar: SPF, DKIM, DMARC; bila perlu, daftar hitam dan/atau daftar putih dapat diatur untuk domain tertentu
- Apabila memungkinkan, surel eksternal harus ditandai sebagai "EKSTERNAL"

DAN INGAT

Penipu tidak hanya dapat mengambil alamat surel dari koresponden Anda, tetapi juga alamat surel Anda. Ia mengirimkan jawaban yang ia terima dari pihak lawan bicara Anda, dan juga sebaliknya. **Ilusinya sempurna**

RISIKO SIBER

PHISHING DAN *SPEAR PHISHING*

CONTOH

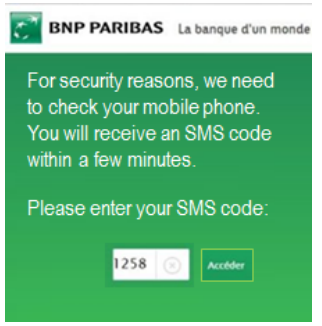
Anda menerima surel yang tampaknya berasal dari bank Anda. Apabila Anda klik tautannya, halaman bank palsu terbuka dan meminta informasi (kata sandi, nomor kartu kredit, dll.). Penipu juga dapat mencuri kode SMS yang dikirimkan oleh bank Anda untuk memvalidasi rekening atau pembelian kartu.

Anda menerima pesan baru

J **john@bnpparibas.com** Today at 9:02 AM

À : kate@qwerty-analysis.com

Nasabah yang terhormat,
Anda memiiliki 2 pesan baru. Periiksa kotak masuk anda dengan mengklik tautan dibawah:
Your mailbox



Phising sangat umum terjadi, dan dapat memengaruhi **perusahaan telepon, pemasok listrik atau gas Anda, administrasi, penyedia surel** (Gmail, Hotmail...), media sosial, dan lainnya..

Info: kami menerima permintaan kartu SIM baru untuk kontrak telepon seluler Anda. Apabila Anda tidak bertanggung jawab atas permintaan ini, harap segera hubungi Help Desk di 12345

Penipu juga dapat **mencuri kode yang dikirimkan melalui SMS oleh bank Anda** dengan meminta kartu SIM baru yang dikirim oleh operator telepon Anda. Ini dikenal sebagai *SIM swapping*.

TANDA-TANDA PERINGATAN

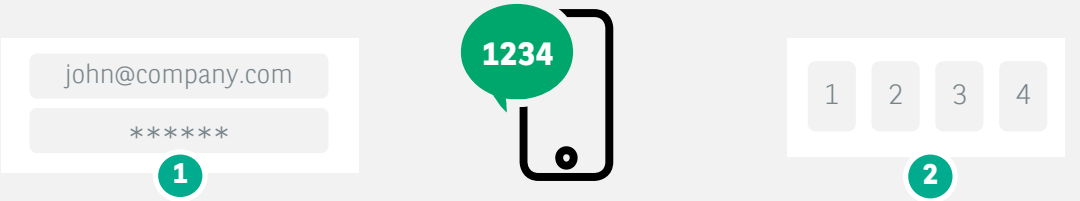
- Surel **yang tampaknya berasal dari institusi** yang memiliki hubungan dengan Anda (LinkedIn, bank, pemasok, nasabah, otoritas pajak...), dengan tautan atau lampiran
- **Permintaan tidak terduga** yang tampaknya memiliki dasar logis (faktur...)
- **Pesan yang mengkhawatirkan atau menghasut** yang mendesak Anda untuk membuka atau mengklik berkas
- **Ketidaksesuaian apa pun** dalam surel (ejaan...)

LINDUNGI DIRI ANDA

Kembangkan refleks yang tajam!

- Periksa **perihal** dan **isi** surel dengan cermat (ejaan, pesan yang mengkhawatirkan...), **serta alamat surel pengirim**, terutama *domain*
- Sebagai aturan umum, **jangan buka lampiran dan jangan klik tautan apa pun atau gambar yang dapat diklik** yang diberikan dalam surel yang Anda terima
- Untuk mengakses sarana perbankan atau aplikasi media sosial Anda, selalu gunakan aplikasi asli atau gunakan Favorit atau masukkan alamat yang biasa ke peramban Anda; cek keberadaan **https://** dan **ikon gembok**
- Apabila Anda tidak sengaja mengklik tautan dalam surel, jangan masuk di situs web tersebut: jangan masukkan kata sandi, atau kode yang dikirimkan melalui SMS
- Jangan buka atau balas surel yang mencurigakan; jangan hubungi nomor telepon yang diberikan dalam surel ini

Gunakan otentikasi yang kuat di situs perbankan web Anda. Aktifkan otentikasi 2-langkah di Gmail, Hotmail, LinkedIn, Facebook, Apple...



DAN INGAT

- Apabila Anda mengalami **masalah pada ponsel Anda** (kehilangan jaringan dalam jangka waktu lama, kartu SIM tidak valid), Anda mungkin menjadi korban SIM *swapping*; hubungi operator telepon Anda
- ***Spear phising*** adalah serangan phising yang diarahkan ke individu atau perusahaan tertentu untuk mencuri data, memasang *malware*, dll; pengirim mungkin terlihat seperti seseorang yang Anda kenal
- **Cek tautan dengan mengarahkan pada URL**; alamat penerusan ditampilkan pada bagian bawah navigator Anda)

INFEKSI PERANGKAT LUNAK BERBAHAYA (*MALWARE*)

CONTOH

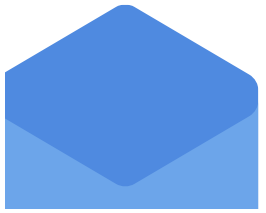
***Malware* (*malicious software infection*) adalah perangkat lunak perusak yang dipasang secara tidak sengaja dan tanpa Anda ketahui, biasanya dengan mengklik suatu tautan atau membuka dokumen.**

Tagihan belum dibayar - Penting

SC **Accounting department** Today at 9:02AM

À : kate@qwerty-analysis.com

Dengan memeriksa akun Anda, kecuali kami keliru, pembayaran faktur F00012 kami sebesar €300 belum diterima. Anda dapat mengunduh salinan faktur di alamat ini:
Unduh tagihan
Kami mohon Anda untuk menyelesaikannya sesegera mungkin.



Tagihan belum dibayar

SC **Accounting department** Today at 9:02AM

À : ,jjjj

I00012.doc
29 Kb

Halo,
Terlampir adalah faktur yang masih menunggu pembayaran sejumlah €1927.80.

TANDA-TANDA PERINGATAN

- Surel apa pun **dari kontak yang tidak dikenal** dengan tautan atau lampiran
- Surel apa pun dengan **perihal yang tidak biasa atau isi yang menarik**
- Berkas apa pun yang dikirimkan melalui surel atau yang diunduh, memuat makro yang melekat

PERINGATAN: Kita semua bisa menjadi korban infeksi malware. Konsekuensinya bisa sangat serius: Spionase, pencurian data, transfer palsu, enkripsi data perusahaan yang mengarah pada penyuapan dan kemungkinan kerugian operasional.

LINDUNGI DIRI ANDA

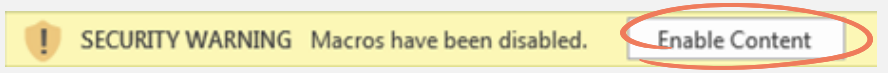
Pada saat menerima surel

- Apakah Anda kenal pengirimnya? Apakah itu alamat biasanya? Apakah Anda mengharapkan surel ini? Apakah perihal atau pesannya tidak biasa?
- Apabila ragu-ragu, **jangan buka lampiran atau tautannya**
- Surel penipuan bisa berasal **dari salah satu kontak Anda** yang biasa, apabila peralatan kerjanya telah terinfeksi; jika ragu-ragu, hubungi dia

Apabila Anda membuka lampiran atau mengunduh file:

- Lakukan di stasiun kerja yang dilindungi oleh antivirus, bukan di smartphone Anda
- Jangan aktifkan isi atau izinkan eksekusi makro

Jangan diklik!



Lindungi sistem komputer Anda

- Perbaharui sistem operasi dan antivirus Anda **setiap hari**
- **Batasi hak instalasi perangkat lunak** untuk administator
- Jangan izinkan **eksekusi makro** atau membuka lampiran secara otomatis
- **Blokir stik USB** dan situs berbagi file
- **Filter lampiran** yang berisi kode Visual Basic (makro)
- Cek keamanan **Protokol Desktop Jarak Jauh** (VPN atau kata sandi yang kuat) dan waspadai **pelanggaran keamanan situs web** (misal: formulir kontak)
- Hindari berselancar di situs web yang tidak **dikenal**
- Apabila memungkinkan, **segmentasikan** jaringan komputer Anda

DAN INGAT

- Perangkat lunak antivirus seringkali **tidak mendeteksi malware**
- Penipu sering menggunakan tautan yang meneruskan ke berkas yang disimpan di DropBox, Google Drive, ... atau di situs web UKM yang diretas, untuk melawan filter
- Semakin banyak *malware*/trojan yang dapat berjalan di komputer Anda tanpa tindakan apa pun dari Anda bahkan hanya dengan mengunjungi situs web dengan keamanan yang rentan

PENIPUAN *MALWARE* "PERBANKAN"

CONTOH

Malware **dapat melakukan transfer di situs perbankan Anda. Khususnya, *malware* dapat menampilkan halaman validasi palsu untuk mencuri kode validasi:**

Halaman masuk ASLI

BNP PARIBAS

Masuk ke rekening Anda

Kode pelanggan

12345678

Kode akses anda

******

Masuk

Halaman palsu: permintaan validasi untuk login

BNP PARIBAS

PENIPUAN

Masuk ke rekening Anda

Untuk melanjutkan validasi

1. Masukkan kode tantangan pada pembaca Anda, dan masukkan kode PIN Anda
2. Masukkan kode respons dan konfirmasi

Kode tantangan: 9876 5432

******

Konfirmasi

TANDA-TANDA PERINGATAN

- **Halaman validasi** tidak biasa, atau muncul setelah periode ketidaktersediaan alat perbankan
- Kegagalan autentikasi yang berurutan dan **berpotensi abnormal**
- **Pelambatan**, lalu lintas jaringan yang sangat tinggi, aktivitas diska yang lebih tinggi dan/atau perubahan berkas dapat menjadi tanda adanya infeksi pada perangkat keras Anda

LINDUNGI DIRI ANDA

Gunakan aplikasi pembayaran Anda dengan sebaik-baiknya

- Jangan terhubung jika ada dugaan peretasan atau *malware*; jika ragu, hubungi **Relationship Manager** Anda
- **Keluar** dari aplikasi Anda dan hapus alat validasi Anda setelah setiap sesi. Hapus juga data navigasi yang muncul di peramban Anda
- Jangan pernah mengungkapkan **ID, kata sandi, kode validasi,** dll. kepada siapa pun, dengan cara apa pun
- Hindari terhubung dengan **PC atau ponsel pribadi** atau dengan **jaringan *Wi-Fi* publik**
- Apabila Anda menggunakan berkas transfer pembayaran, hindari langkah-langkah manual sebisa mungkin (untuk mencegah penjahat mengubah berkas pembayaran)
- Apabila memungkinkan, lakukan pembayaran di PC khusus hanya untuk tujuan tersebut

Pembagian tugas

- Selalu pastikan setidaknya ada kontrol ganda pada pembayaran dan manajemen vendor Anda
- Pemisahan tugas tidak 100% aman terhadap *malware* perbankan, tetapi seringkali efektif

Lindungi instalasi TI Anda

- Perbarui sistem operasi dan antivirus Anda **setiap hari**
- Lihat tips lain di halaman 18

DAN INGAT

- Deliotte: "Ketika kami melakukan **tes instrusi**, kami dapat mengakses sistem perbendaharaan di 80% kauss; kecuali semuanya dienkripsi, biasanya memungkinkan untuk mengubah jumlah dan rincian rekening pemasok"
- Solusi pengawasan pembayaran "***Secure Flows***" memberikan tambahan kontrol atas negara dan rekening tambahan yang tidak terikat dengan sistem informasi Anda; solusi ini tersedia di Prancis dan akan diluncurkan di negara lain

SEBUAH RISIKO BESAR: *RANSOMEWARE*

CONTOH

Malware spreads across your computer network, and encrypts all files. It displays a message demanding the payment of a ransom, in exchange for a cryptographic key to decrypt your data.

TANDA-TANDA PERINGATAN

- **Kecurigaan terhadap infeksi *malware*** apa pun (contoh: makro dalam dokumen yang dicurigai telah dieksekusi oleh karyawan...)
- Suatu halaman memberi tahu Anda **bahwa data Anda telah dienkripsi**

LINDUNGI DIRI ANDA

Dalam hal terjadi serangan

- **Putuskan sambungan semua PC** dari jaringan untuk menghentikan serangan
- Pihak yang berwenang sangat menyarankan untuk **tidak membayar uang tebusan apa pun**

Pencegahan

- Buat cadangan data penting secara rutin
- **Kontrol akses ke direktori penyimpanan cadangan secara ketat** (*ransomeware* mungkin mengenkripsi cadangan)
- Simpan cadangan yang terputus secara rutin
- **Uji** cadangan Anda secara rutin

Susun rencana tindakan dalam hal terjadi serangan

- Bicarakan terlebih dahulu dengan **manajer TI** Anda
- Rencanakan rencana cadangan untuk **proses penting** Anda
- Apabila memungkinkan, belilah asuransi siber, yang melingkupi bantuan ahli, kerugian operasional, dll serta memberi Anda akses ke **dukungan ahli** 24/7

DAN INGAT

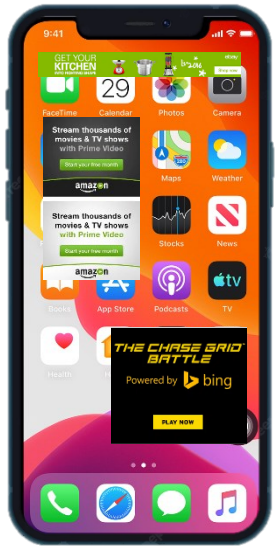
- Terkadang penipu mengancam akan **mengungkapkan data yang disusupi ke publik** apabila korban tidak membayar tebusan
- Secara umum, biaya dari suatu serangan paling sedikit **€40,000**; jumlah kerugian tertinggi sampai dengan ratusan juta euro

PONSEL PINTAR: SASARAN BARU

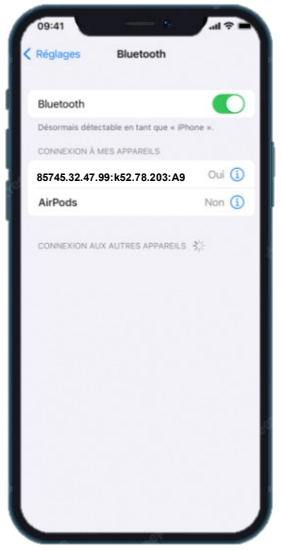
CONTOH

Android, IOS, WinPhone: OS ponsel pintar apa pun benar-benar aman. Ponsel pintar kita memiliki banyak informasi rahasia (SMS, Surat, Foto, Media sosial dll.) dan seringkali tidak memiliki pertahanan, menjadi tambang emas bagi peretas!

Contoh *ransomware*



Contoh *adware*



Contoh peretasan jaringn

TANDA-TANDA YANG HARUS MEMBUAT ANDA WASPADA

- **Iklan yang ada** di ponsel pintar Anda di luar aplikasi Anda
- **Perangkat *Bluetooth* tak dikenal** yang terdaftar di ponsel pintar Anda
- Aplikasi yang **dipasang** di luar toko resmi
- **Panggilan atau pesan** tidak biasa di log Anda

LINDUNGI DIRI ANDA

- **Hindari risiko**
  - Jangan pernah mengunduh aplikasi di luar toko resmi (Apple Store, Play Store)
  - Jangan pernah menjalankan pernah file: .apk, .ipa, .script dll... pada ponsel pintar Anda
  - Non-aktifkan fungsi NFC, Bluetooth dan Infrared setelah menggunakannya (untuk ponsel yang kompatibel)
  - Jangan isi daya ponsel Anda di terminal USB layanan mandiri
  - Periksa keabsahan akses data aplikasi
  - Selalu aktifkan otentikasi dua-faktor (2FA) apabila memungkinkan
  - Jangan melakukan *jailbreak* pada ponsel Anda
- **Jika serangan terjadi**
  - Beri tahu siapa pun yang mungkin telah menerima pesan tipuan dari ponsel Anda
  - Ubah kata sandi applikasi sensitif (perbankan, media sosial dll.)
  - Segera hubungi dukungan merek ponsel Anda
- **Susun rencana tindakan dalam hal terdapat serangan**
  - Lakukan pencadangan secara rutin terhadap data penting Anda
  - Jangan simpan data sensitif atau kata sandi pada ponsel pintar Anda
  - Hindari *wi-fi* publik atau jaringan internet tidak terlindungi sebisa mungkin (atau gunakan VPN)

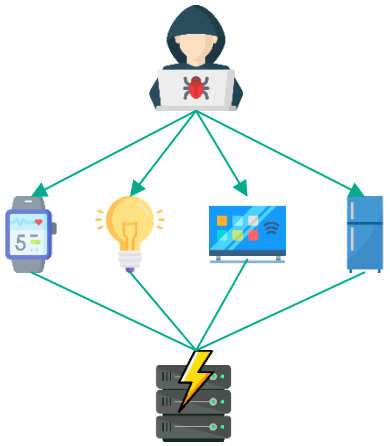
DAN INGAT

- 1 dari 36 ponsel pintar Android memiliki applikasi berisiko yang terpasang (di seluruh dunia)
- Di awal tahun 2022, penemuan teknik “Noreboot” pada iPhone yang memungkinkan peretas untuk mengendalikan kamera dan mikrofon secara jarak jauh dari ponsel pintar tersebut tanpa terdeteksi

OBJEK YANG SALING TERHUBUNG, PINTU TERBUKA BAGI PERETAS

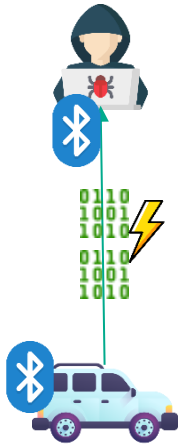
CONTOH

Dalam beberapa tahun terakhir, IOT (*Internet of Things;* Internet untuk Segala) telah menyerbu rumah kita. Kekhasan dari perangkat ini: mereka terhubung langsung dengan Internet. Kami dapat menemukan televisi, jam tangan, speaker, kamera keamanan, lampu, lemari es, monitor bayi dll. Namun, perangkat ini sering kali tidak memiliki sistem keamanan!



Serangan DDoS

Pendengar Aktif



Pencurian Data (Blueborne)

TANDA-TANDA YANG HARUS MEMBUAT ANDA WASPADA

- Penggunaan intensif perangkat Anda meskipun ketika perangkat tidak digunakan (panas)
- Aktivitas anomaly pada kotak internet Anda (peningkatan konsumsi internet)
- Perubahan perilaku pada objek yang terhubung (perubahan bahasa, kesalahan, dll.)
- Tiba-tiba berkas terenkripsi di perangkat Anda

LINDUNGI DIRI ANDA

- **Hindari risiko**
  - Non-aktifkan akun demo atau tamu dari objek yang terhubung
  - Ubah kata sandi IOT asli dengan kata sandi yang kuat
  - Terapkan metode enkripsi jika memungkinkan
  - Hindari untuk menghubungkan komputer profesional Anda ke jaringan dengan IOT, jika tidak, gunakan VPN yang disediakan oleh perusahaan Anda
  - Perbarui perangkat Anda secara rutin untuk memperbaiki kerentanan
- **Dalam hal serangan terjadi**
  - Putuskan sambungan perangkat Anda dari internet untuk menghentikan serangan
  - Ubah kata sandi perangkat Anda
  - Lakukan pencarian pembaruan untuk *patch* keamanan terbaru

DAN INGAT

- IOT Anda memiliki, seperti komputer Anda, alamat IP yang dapat dilihat semua orang di web. Pemindaian IP sederhana di internet dapat menemukan jutaan objek terhubung yang tidak terlindungi
- Situs web Shodan dapat menemukan semua objek terhubung dengan alamat IP yang dapat dilihat di internet (oleh karena itu tidak terlindungi)
- Situs web Insecam memberikan akses ke ribuan kamera tidak terlindungi di dunia dan kemampuan untuk berkonsultasi dengan mereka kapan saja

Bahkan perangkat terhubung yang paling tidak berisiko sekalipun dapat diserang. Ini kasus di tahun 2020 dengan gelombang ransomware yang menginfeksi mesin kopi terhubung yang sehingga tidak dapat digunakan jika pemiliknya tidak membayar tebusan.

KESIMPULAN

KEMBANGKAN REFLEKS YANG TAJAM & GUNAKAN AKAL SEHAT!

Dalam hal permintaan transfer kredit yang tidak biasa

- Beri tahu Manajemen Seniro
- Selalu ikuti proses hukum yang wajar, terlepas dari keadaan darurat yang dirasakan
- Ikuti prinsip pemisahan tugas
- Periksa identitas korensponden Anda menggunakan **rincian kontak yang diverifikasi**

Dalam hal modifikasi rincian bank pemasok

- Periksa identitas koresponden Anda menggunakan **rincian kontak yang diverifikasi**
- Periksa juga apabila terdapat **modifikasi rincian kontak**
- Apabila akun berdomisili di luar negeri, dan untuk **pemasok terbesar** Anda, bersikaplah ekstra waspada

Dalam hal teknisi ingin membantu

- Hubungi **Relationship Manager** Anda (atau vendor perangkat lunak) menggunakan rincian kontak yang diverifikasi
- Jangan berikan **akses jarak** jauh ke PC Anda
- **Jangan pernah melakukan tes pembayaran** lebih dari € 1
- Jangan pernah berikan kode apa pun

Dalam hal permintaan informasi

- Jangan pernah berikan informasi kepada **orang yang tidak Anda kenal**
- Hati-hati apabila seseorang meminta **informasi akuntansi** kepada Anda
- Periksa identitas kontak Anda menggunakan rincian kontak yang diverifikasi, atau melalui pusat data

Di media sosial dan di luar perusahaan

- Bersikaplah bijaksana di **media sosial** dan di luar perusahaan Anda, mengenai peran dan fungsi Anda
- Jangan publikasikan **informasi yang berguna** bagi penipu (bagan, berita tentang perjalanan CEO, templat surat, tanda tangan...)
- Apabila memungkinkan, gunakan **tanda tangan berbeda** untuk perintah bank dengan yang tersedia di dokumen yang tersedia secara publik

Dalam hal menerima surel

- Periksa dengan teliti **perihal, isi dan alamat surel** pengirim
- Jangan klik tautan di surel: selalu gunakan applikasi atau situs web asli, jika tidak sengaja mengklik tautan di surel, **jangan masukkan informasi apa pun**
- Jika memungkinkan, jangan buka lampiran atau mengunduh berkas: jika Anda membuka berkas, **jangan mengaktifkan konten atau menjalankan makro**

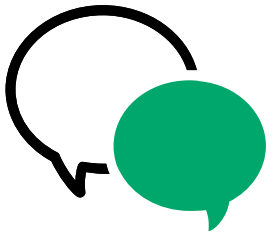
Ketika menggunakan aplikasi perbankan Anda

- **Pisahkan tugas**, gunakan jumlah pembatasan, jangan gunakan perintah dan validasi kertas
- Hindari terhubung dari **PC pribadi** atau ponsel pintar atau jaringan **Wi-Fi publik**
- **Keluar** dari aplikasi Anda dan hapus sarana validasi Anda setelah setiap sesi
- Jangan masuk ketika ada *malware* dicurigai (halaman validasi palsu, kegagalan yang tidak biasa...); jika ragu-ragu, hubungi **Relationship Manager** Anda

Lindungi instalasi TI Anda

- **Perbahaarui** O.S dan antivirus setiap hari
- Keamanan **RDP** (VPN atau kata sandi)
- Keamanan **situs web** (formulir kontak)
- Jika memungkinkan, **pisahkan** jaringan komputer Anda
- **Blokir stik USB** & situs berbagi berkas
- **Filter surel** dan lampiran, dan cek otentikasi surel (SPF, DKIM, DMARC)
- Lakukan **pencadangan** rutin dan teruji
- Lihat domain yang **mirip** dengan milik Anda
- Jika memungkinkan, enkripsikan data sensitif dan gunakan TLS untuk surel eksternal

DALAM HAL PENIPUAN TRANSFER PALSU TERJADI (ATAU KECURIGAAN)



1

Beritahukan manajemen Anda dan simpan bukti

DAFTAR PANGGILAN DARURAT

2

Hubungi Relationship Manager Anda segera

DAFTAR PANGGILAN DARURAT

3

Hubungi polisi dan ajukan pengaduan jika terjadi penipuan yang berhasil

DAFTAR PANGGILAN DARURAT

Penafian

Isi dari dokumen ini bersifat umum dan bukan merupakan nasihat hukum, keuangan, pajak atau profesional. Meskipun informasi yang dimuat dalam dokumen ini telah diperoleh dari sumber-sumber yang diyakini PT Bank BNP Paribas Indonesia dapat diandalkan, tidak ada pernyataan atau jaminan apa pun, tegas maupun tersirat, yang dibuat dan tidak ada tanggung jawab apa pun yang diterima atau akan diterima oleh PT Bank BNP Paribas Indonesia mengenai atau dalam kaitannya dengan keakuratan, keandalan atau kelengkapan dari informasi tersebut. Semua dan setiap tanggung jawab dan kewajiban tersebut secara tegas dan sepenuhnya disangkal.

Pendapat-pendapat yang dinyatakan dalam dokumen ini mencerminkan penilaian PT Bank BNP Paribas Indonesia pada tanggal dokumen ini dan dapat tunduk pada perubahan tanpa pemberitahuan apabila PT Bank BNP Paribas Indonesia mengetahui informasi apa pun, yang bersifat khusus ataupun umum, yang mungkin memiliki dampak material terhadap pendapat-pendapat tersebut.

Baik PT Bank BNP Paribas Indonesia maupun setiap afiliasinya atau direktur, pejabat atau karyawan masing-masing tidak bertanggung jawab atas setiap kerugian atau kerusakan yang diderita atau dialami oleh pihak mana pun akibat mengandalkan atau menggunakan dokumen ini.

Tidak ada hal apa pun dalam dokumen ini yang akan ditafsirkan sebagai pemberian atau penyerahan hak apa pun melalui lisensi atau sehubungan dengan setiap paten, hak cipta, merek dagang atau logo Grup BNP Paribas (termasuk pengetahuan teknis dan rahasia dagang) atau hak kekayaan intelektual lainnya.

Dokumen ini tidak dapat diproduksi kembali (secara keseluruhan maupun sebagian) dan tidak dapat diringkas atau didistribusikan tanpa persetujuan tertulis sebelumnya dari PT Bank BNP Paribas Indonesia.

PT Bank BNP Paribas Indonesia diatur dan diawasi oleh Otoritas Jasa Keuangan sebagai bank umum. Informasi dalam dokumen ini tidak dimaksudkan untuk didistribusikan kepada, atau digunakan oleh, atau bukan merupakan penawaran apa pun kepada, setiap orang atau badan di yurisdiksi manapun apabila (a) pendistribusian atau penggunaan atau penawaran informasi tersebut akan bertentangan dengan hukum atau peraturan, atau (b) PT Bank BNP Paribas Indonesia akan menjadi tunduk pada persyaratan hukum atau peraturan yang berlaku.

Dengan menerima dokumen ini, Anda sepakat untuk terikat pada pembatasan-pembatasan tersebut di atas.