



Defenxor Intelligence Managed Security

Pengenalan dan Pencegahan *Mail Phishing*



Mail Phishing

Apa itu Phishing?

Phishing adalah jenis ancaman online di mana penjahat menyamar sebagai organisasi yang sah melalui media email, pesan teks, iklan, atau cara lain untuk mencuri informasi sensitive atau menyebarkan malware.

Hal ini biasanya dilakukan dengan menyertakan tautan mengarah ke suatu situs palsu dan meminta target korban memasukkan informasi sensitifnya atau menginstall software yang mengandung malware.



Tujuan dari serangan phishing



Pencurian Identitas
(NIK,NIP,NPWP,dll)



Kredensial
(username, dan password)



Informasi Keuangan

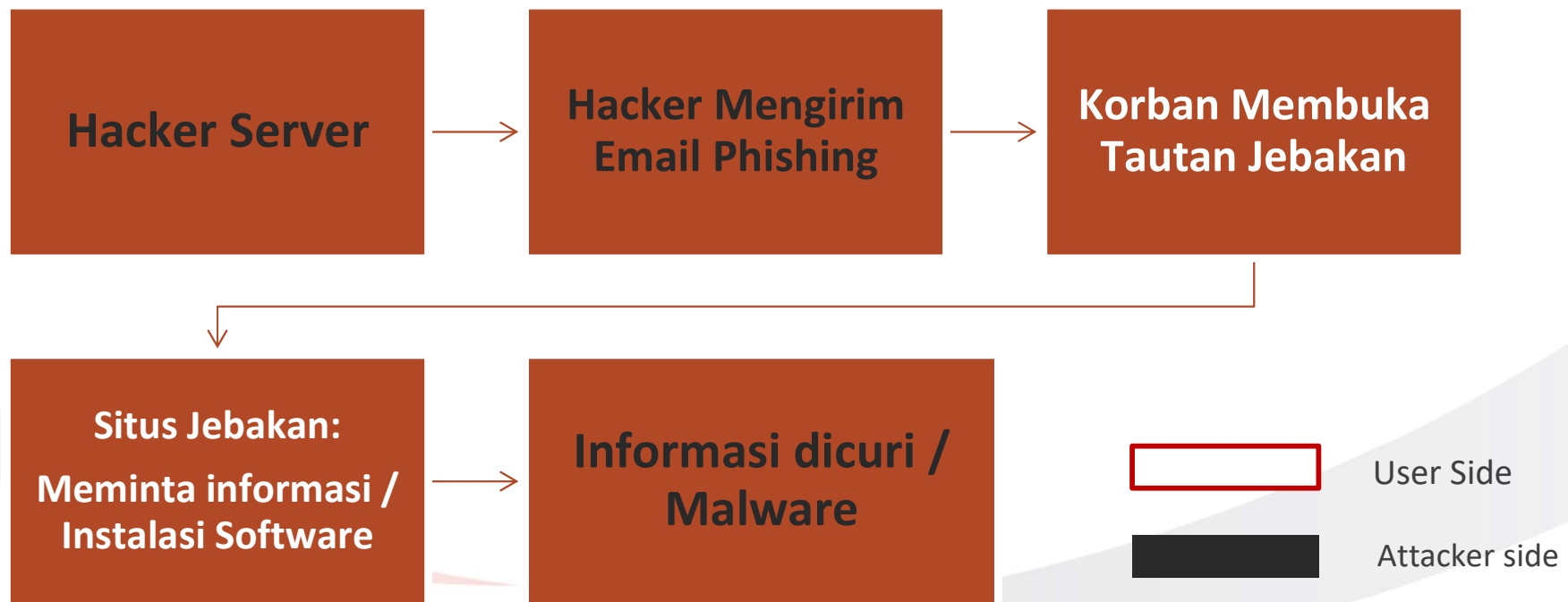


Infeksi Malware



Transfer Uang

Cara Attacker Menyebarkan Mail Phishing



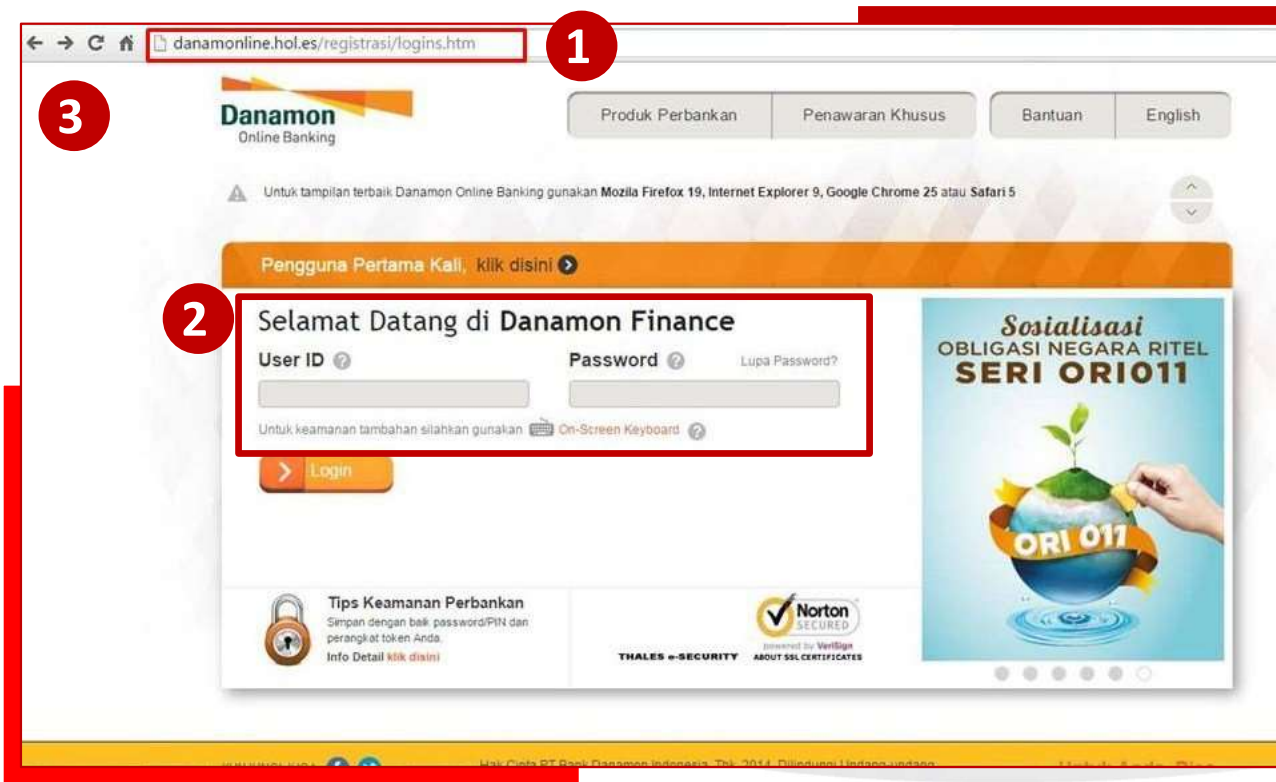
Penyebab aktivitas Phishing yang Berhasil

- 1** | Adanya rasa takut (email phishing berisi peringatan/ancaman) sehingga timbul rasa panik lalu membuka isi phishing tersebut
- 2** | Adanya urgensi mengenai kebutuhan yang berkaitan dengan isi ataupun subject phishing
- 3** | Rasa senang ketika mendapatkan Phishing dengan pesan yang menggembirakan
- 3** | Mudah percaya ketika mendapatkan Phishing hadiah yang cukup besar dan cukup menjanjikan



Contoh Kasus Mail Phishing

Contoh Link Phishing



1 Domain tidak Official

2 Terdapat form untuk mendapatkan informasi yang dibutuhkan oleh attacker

3 Tampilan dibuat semirip mungkin dengan official web

Contoh Mail Phishing

From: myAt&t ddt34@fhgvh876.com
To: "att-services.123085063@att-mail.com" att-services.123085063@att-mail.com
Sent: Saturday, August 1, 2020, 7:08:50 AM EDT
Subject: Upgrade Now

myAT&T

Upgrade now before you lose your email account

The Classic version of your Mail will be replaced by our new version on the 3rd of August 2020. So it's time to upgrade before you lose your email access.

[UPGRADE NOW](#)

Protecting your information is important to us and we work continuously to strengthen the threats targeting our Financial Institution.

Thanks for choosing us,
AT&T

1 Domain tidak Official

2 Penggunaan kalimat bahasa yang buruk

3 Signature mail terlalu umum (dalam hal ini signature hanya AT&T tidak spesifik siapa yang mengirimkan mail)

Contoh Mail Phishing



Halo,

Peringat Terakhir: Email ini menginformasikan bahwa kiriman Anda masih dalam proses.

Paket Anda tidak dapat dikirim pada 15.03.2021 karena tidak ada bea masuk yang dibayarkan **36.14 (Rp)**

Merchant: Pos Indonesia
Referensi: 20211802-15470
Uraian pesanan: Biaya transportasi
Jumlah: 36.14 (Rp)
Pengiriman dijadwalkan antara: 16.03.2021 - 17.03.2021



Untuk mengkonfirmasi pengiriman paket Anda [Klik di sini](#).

Terima kasih atas kepercayaan Anda,

Hormat kami,
Layanan pelanggan [Pos Indonesia](#) Anda.

Hak Cipta © 2005-2021 EMS Indonesian Post, Semua Hak Dilindungi Undang-Undang

Pos Indonesia mengoperasikan jaringan layanannya ke lebih dari 17.000 pulau di seluruh Indonesia. Untuk menjaga kinerja pelayanan, sistem transportasi menjadi perhatian yang sangat dalam. Untuk angkutan surat sebagian besar, Pos Indonesia mengandalkan kemitraan dengan pihak lain seperti kereta api, Operator bus, pesawat dan kapal baik milik pemerintah maupun swasta. Namun, waktu pengiriman dan konektivitas transportasi ditetapkan untuk mencapai standar Universal Postal Union (UPU).



Nomor kartu:	Nama di kartu:
<input type="text"/>	<input type="text"/>
Tanggal habis tempo:	CVV2/CVC2:
<input type="text" value="Bulan"/> <input type="text" value="tahun"/>	<input type="text"/>

Jumlah order: 20211802-15470
Uraian pesanan: Biaya transportasi

Pos Indonesia

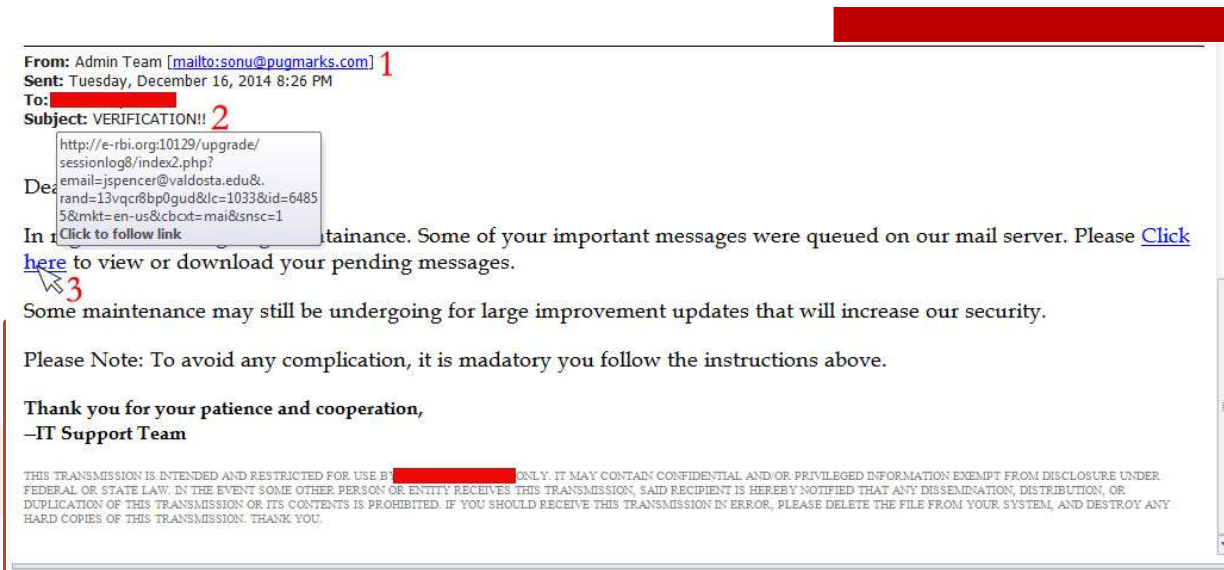
☐ Terima syarat dan ketentuan

Total: **36.14**_(Rp)

Pembayaran online



Contoh Mail Phishing



- 1 Domain tidak Official
- 2 Penggunaan Subject yang kurang jelas
- 3 Terdapat clicked link yang unofficial dan juga mencurigakan



Pencegahan adanya Mail Phishing

Pencegahan adanya Mail Phishing

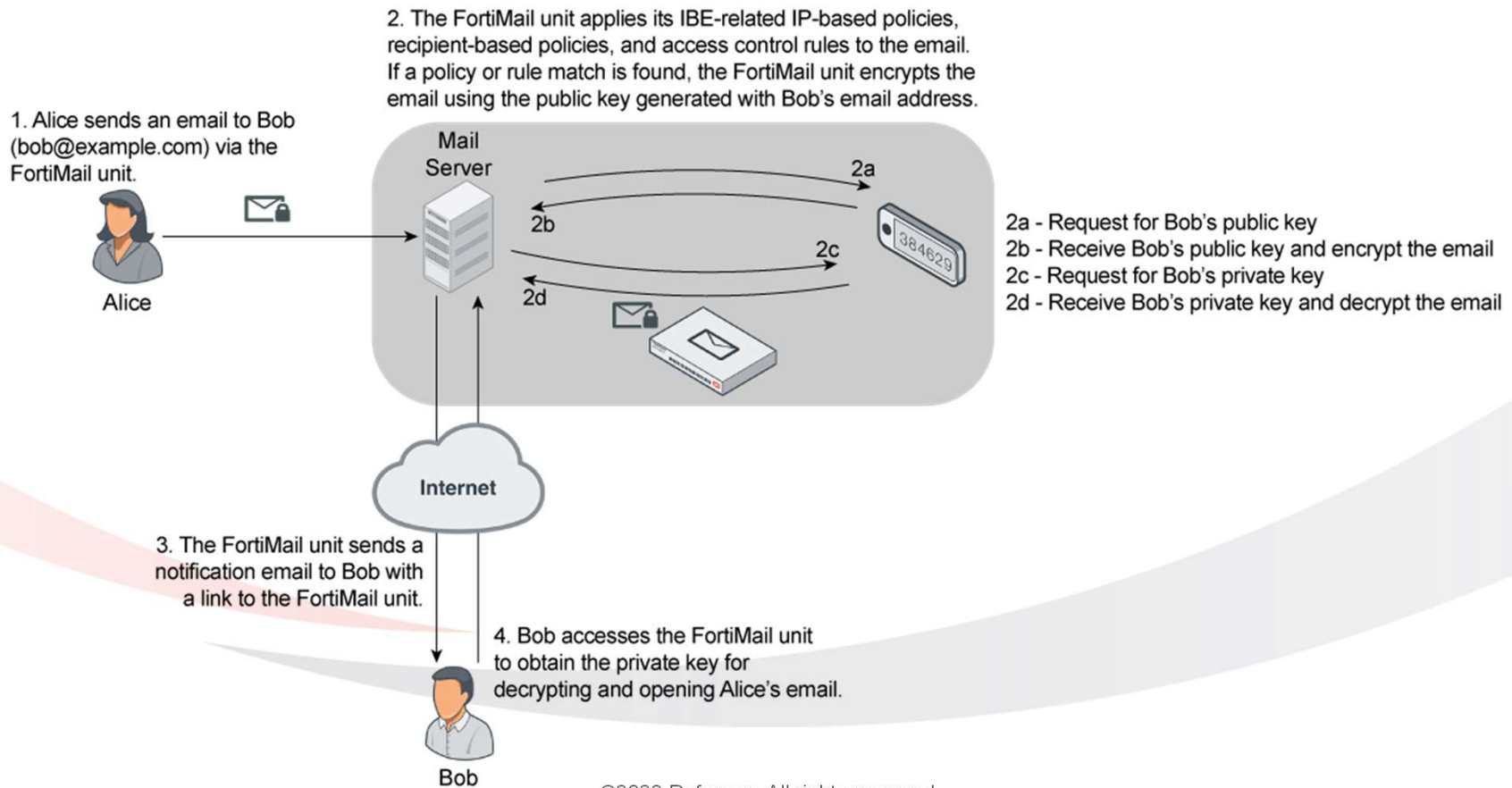
Pengguna

- 1** | Periksa alamat email pengirim, bukan hanya dari namanya saja. Periksa link yang terdapat di email, apakah URLnya valid dan benar?
- 2** | Jangan download maupun klik link yang tertera pada email tanpa melakukan verifikasi keaslian pengirimnya.
- 3** | Hati-hati Terhadap Tata Bahasa Pesan Email Yang Buruk
- 4** | Mewaspada pesan mengenai hal – hal yang tidak masuk akal untuk menjadi kenyataan

Security Engineer

- 1** | Melakukan konfigurasi dan pembuatan rules pada perangkat Mail Security
- 2** | Menetapkan policy terkait SPF, DKIM, dan DMARC
- 3** | Melakukan review secara berkala terhadap rules yang sudah dibuat

Investasi Keamanan dengan Mail Security



Periksa emailmu apakah pernah bocor ?

<https://haveibeenpwned.com/>



Human error was a major contributing cause in 95%
of all breaches.

— IBM Cyber Security Intelligence Index Report



Kesadaran Pengguna dan Dukungan Manajemen

Kesadaran Pengguna akan Keamanan Informasi

" **Pemahaman** dan **apresiasi** dari pengguna akan kebutuhan, tujuan dan manfaat dari keamanan informasi, dan **memberikan komitmennya** terhadap hal tersebut."

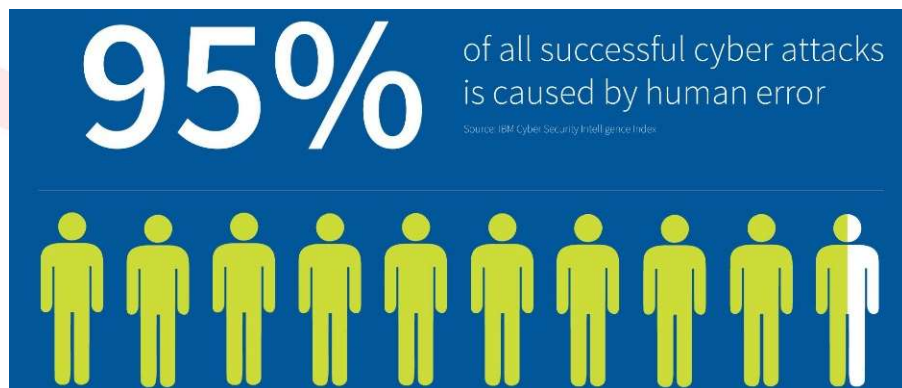
Mengapa Kesadaran Pengguna Penting?

Orang adalah mata rantai terlemah

Tidak semua pengguna IT adalah orang IT

To many work, To complicated >> don't care

Orang adalah target utama serangan



Indikator Kesadaran Pengguna



Karyawan mematuhi kebijakan keamanan



Karyawan mengikuti prosedur penggunaan komputer yang aman



Secara keseluruhan, sadar akan potensi keamanan informasi dan dampak negatifnya



Jumlah insiden keamanan akibat dari perilaku pengguna



Pengguna memproteksi keamanan data-datanya

Dukungan Manajemen akan Keamanan Informasi

"**Dukungan** dan **komitmen** Manajemen, terhadap kegiatan, inisiatif serta kebutuhan lainnya untuk meningkatkan keamanan informasi dari perusahaan."

Mengapa Dukungan Manajemen Penting?

- Memberikan dampak paling besar
- Karena IT saat ini di level strategis, maka IT Security juga
- Harus melibatkan level tertinggi?

The image is a screenshot of a Forbes article. On the left, there is a vertical sidebar with icons for a menu, search, settings, and a '2 TOP COMMENTS' button. The main content area shows the Forbes logo and 'Entrepreneurs' section. The article title is 'Target CEO Fired - Can You Be Fired If Your Company Is Hacked?'. Below the title is a profile picture of Eric Basu, a contributor. The article text begins with 'A common perspective is that cyber security is primarily the responsibility of the IT department. If a data breach incident occurred, the senior IT executive was the only one to take the fall, and usually only if there was incompetence involved vs. simply bad luck.' At the bottom, there is a disclosure statement: 'Legally required disclosure statement: My company, Sentek Global, provides some of the services referred to in this article.'

Forbes / Entrepreneurs

JUN 15, 2014 @ 8:00 PM 18,139 VIEWS

Target CEO Fired - Can You Be Fired If Your Company Is Hacked?

Eric Basu
CONTRIBUTOR

I offer a military and cyber security perspective on entrepreneurship **FULL BIO**
Opinions expressed by Forbes Contributors are their own.

FOLLOW

A common perspective is that cyber security is primarily the responsibility of the IT department. If a data breach incident occurred, the senior IT executive was the only one to take the fall, and usually only if there was incompetence involved vs. simply bad luck.

Legally required disclosure statement: My company, Sentek Global, provides some of the services referred to in this article.

10 Stocks to Buy NOW

Seperti Apa Dukungan Manajemen ?

01

Pembentukan Kebijakan dan
Prosedur Keamanan Informasi

02

Dukungan terhadap fungsi atau
satuan kerja Keamanan Informasi

03

Dukungan dalam investasi pada
keamanan informasi

04

Dukungan terhadap pelatihan
Keamanan Informasi



Stay Safe