

Reading Material

**Mengimplementasikan Proses Testing - Case study :
Simulasi serangan phishing melalui email untuk
menguji kesadaran keamanan pengguna**



Simulasi serangan phishing melalui email untuk menguji kesadaran keamanan pengguna

Apa itu phising?

Email phishing adalah bentuk serangan siber di mana penyerang mencoba untuk mendapatkan informasi sensitif, seperti kata sandi, informasi keuangan, atau data pribadi lainnya, dengan menyamar sebagai entitas terpercaya melalui email palsu. Tujuannya adalah untuk mengelabui penerima agar mengungkapkan informasi sensitif atau melakukan tindakan tertentu, seperti mengklik tautan berbahaya atau membuka lampiran berbahaya.

Bagaimana Serangan Email Phishing Bekerja?

Pengenalan Penyerang

Penyerang mencari target potensial, baik individu atau organisasi, yang sering kali memiliki data berharga.

Pembuatan Email Palsu

Penyerang membuat email palsu yang terlihat seperti berasal dari entitas terpercaya, seperti perusahaan, lembaga keuangan, atau layanan online populer. Mereka dapat menggunakan logo, alamat email palsu yang mirip, dan gaya bahasa yang menyerupai aslinya.

Teks dan Tautan yang Menipu

Email tersebut berisi teks yang dirancang untuk menarik perhatian atau menciptakan urgensi. Mungkin mengklaim adanya masalah dengan akun , atau menawarkan promosi menarik. Tautan palsu yang terlihat asli juga dapat dimasukkan untuk mengarahkan ke situs web yang tampak sah.

Upaya Mendapatkan Informasi Sensitif

Email phishing akan meminta untuk memberikan informasi sensitif, seperti kata sandi, nomor kartu kredit, nomor jaminan sosial, atau informasi lainnya. Penyerang sering menggunakan tekanan waktu atau ancaman untuk memaksa berbagi informasi tersebut.

Ciri ciri email phishing

Alamat Email Pengirim yang Mencurigakan

Periksa alamat email pengirim secara seksama. Penipu sering menggunakan alamat email palsu atau yang terlihat mirip dengan entitas terpercaya. Perhatikan perbedaan kecil dalam alamat email, seperti huruf yang salah ketik atau domain yang mirip, misalnya "support@googlee.com" daripada "support@google.com".

Kesalahan Ejaan dan Tata Bahasa

Email phishing sering kali berisi kesalahan ejaan, tata bahasa yang buruk, atau frasa yang tidak wajar. Ini dapat menjadi indikator bahwa email tersebut tidak berasal dari sumber yang sah.

Tekstual yang Menciptakan Urgensi atau Ancaman

Email phishing sering menggunakan teks yang menciptakan urgensi atau ancaman untuk membuat terburu-buru mengambil tindakan. Contoh termasuk pernyataan bahwa akun dalam bahaya atau akan kehilangan akses jika tidak bertindak segera.

Permintaan Informasi Pribadi atau Keuangan

Email phishing dapat meminta untuk memberikan informasi pribadi atau keuangan, seperti kata sandi, nomor kartu kredit, nomor jaminan sosial, atau kode keamanan. Perusahaan terpercaya umumnya tidak akan meminta informasi sensitif melalui email.

Tautan yang Menyamar

Penipu sering menyertakan tautan palsu yang terlihat seperti tautan asli. dapat memeriksa tautan tersebut dengan mengarahkan kursor ke atasnya tanpa mengkliknya, dan perhatikan apakah URL sesuai dengan yang seharusnya.

File Lampiran Berbahaya

Email phishing dapat mengandung lampiran berbahaya yang jika diunduh atau dibuka dapat menginfeksi perangkat dengan perangkat lunak berbahaya atau malware.

Tidak Dijanjikan atau Tidak Diminta Email

Jika menerima email yang tidak pernah minta atau tidak terkait dengan aktivitas yang sedang lakukan, itu bisa menjadi indikasi adanya upaya phishing.

Tautan atau Logo yang Tidak Konsisten

Perhatikan apakah logo, tautan, atau tampilan email sesuai dengan gaya biasa dari entitas yang diklaim oleh email tersebut.

Tidak Ada Personalisasi atau Informasi Kontak yang Minim

Email phishing sering kali tidak akan memiliki informasi personalisasi yang spesifik atau informasi kontak yang jelas, seperti nomor telepon atau alamat fisik.

Tidak Berhubungan dengan Aktivitas

Jika email tersebut tidak relevan dengan aktivitas atau layanan yang gunakan, itu mungkin mencurigakan.

Taktik dan Strategi Penipuan Phishing

Manipulasi Emosi dan Urgensi

Penipu menggunakan psikologi manusia dengan menciptakan emosi seperti rasa takut, kecemasan, atau keserakahan dalam email phishing mereka. Mereka dapat mengancam akan menonaktifkan akun, menghapus data penting, atau memberlakukan denda jika tidak segera bertindak. Penipu juga dapat menjanjikan hadiah besar atau peluang yang menarik untuk mendorong merespons dengan cepat tanpa berpikir.

Tautan dan Situs Web Palsu

Penipu sering memasukkan tautan palsu di dalam email mereka yang mengarahkan ke situs web palsu yang terlihat mirip dengan situs asli. Tujuannya adalah untuk meminta memasukkan informasi pribadi atau keuangan, seperti nama pengguna dan kata sandi, pada situs palsu tersebut. Situs web palsu ini sering kali dirancang dengan sangat cermat agar mirip dengan tampilan situs yang sebenarnya, sehingga sulit untuk membedakannya.

Phishing Melalui Lampiran Berbahaya

Penipu sering menyamar sebagai entitas atau individu yang sah, seperti bank, layanan online, atau teman. Mereka dapat menggunakan

informasi publik yang mereka temukan secara online untuk menciptakan email yang tampak meyakinkan dan membuat percaya bahwa email tersebut berasal dari sumber yang sah.

Spear Phishing

Jenis serangan ini lebih terarah dan personal. Penipu melakukan penelitian mendalam tentang target mereka, mengumpulkan informasi dari media sosial atau sumber lainnya. Dengan informasi ini, mereka menciptakan email yang sangat meyakinkan dan pribadi, membuat target cenderung merespons.

Dampak dan Konsekuensi Phishing

Cerita Korban Phising di Olshop: Rugi Rp10 Juta, Lapor Polisi Belum Ada Solusi

Masyarakat perlu berhati-hati mengakses situs yang tak resmi, serta rajin membaca kebijakan mengenai perlindungan data privasi agar tak jadi korban phising.



Bisnis O Senin, 22 Mei 2023 - 18:35 WIB
Penulis: Maymunah Nasution | Editor: Ika Yuniaty

Solopos.com, SOLO — Seorang penjual *online shop* (olshop), Wulan, mengalami trauma atas serangan *phishing* yang pernah terjadi padanya di salah satu *e-commerce*.

Pencurian Identitas

Dampak: Penipu yang berhasil mendapatkan informasi pribadi, seperti nama pengguna, kata sandi, atau nomor jaminan sosial, dapat menggunakan informasi tersebut untuk mencuri identitas. Mereka dapat membuka akun baru, mengajukan pinjaman, atau melakukan kegiatan kriminal atas nama.

Konsekuensi: Pencurian identitas dapat merusak reputasi , menyebabkan kerugian finansial, dan mengakibatkan masalah hukum yang serius.

Kehilangan Data Pribadi dan Keuangan

Dampak: Jika penyerang berhasil mendapatkan akses ke informasi keuangan atau data pribadi , seperti nomor kartu kredit, rekening bank, atau informasi kartu medis, dapat menghadapi pencurian dana atau penyalahgunaan data.

Konsekuensi: Kehilangan dana atau informasi pribadi dapat merugikan secara finansial dan membahayakan privasi.

Penyebaran Malware dan Ransomware

Dampak: Penipu dapat menggunakan tautan berbahaya atau lampiran beracun dalam email phishing untuk menginfeksi perangkat dengan perangkat lunak berbahaya atau ransomware.

Konsekuensi: Malware atau ransomware dapat merusak perangkat , mencuri data , atau mengenkripsi file dan meminta tebusan untuk mendekripsinya.

Kerugian Keuangan dan Reputasi Organisasi

Dampak: Serangan phishing terhadap perusahaan atau organisasi dapat mengakibatkan pencurian informasi sensitif karyawan atau pelanggan, serta merusak reputasi perusahaan.

Konsekuensi: Organisasi dapat menghadapi kerugian finansial akibat denda atau gugatan hukum, serta kehilangan kepercayaan pelanggan.

Cara Menghindari Phishing

Verifikasi Alamat Email Pengirim

Selalu periksa alamat email pengirim dengan seksama sebelum merespons atau mengklik tautan. Pastikan alamat email cocok dengan yang diharapkan dari sumber yang sah.

Jangan Mengklik Tautan Langsung

Jangan mengklik tautan di dalam email, terutama jika merasa mencurigai email tersebut. Alih-alih, arahkan cursor ke tautan untuk melihat URL yang sebenarnya sebelum mengkliknya.

Hati-hati dengan Lampiran

Jangan membuka lampiran dari email yang tidak harapkan atau yang tampak mencurigakan. Lampiran berbahaya dapat mengandung malware atau ransomware.

Jangan Berikan Informasi Sensitif

Tidak pernah memberikan informasi sensitif, seperti kata sandi, nomor kartu kredit, atau nomor jaminan sosial melalui email. Perusahaan sah umumnya tidak akan meminta informasi tersebut melalui email.

Verifikasi dengan Sumber yang Terpercaya

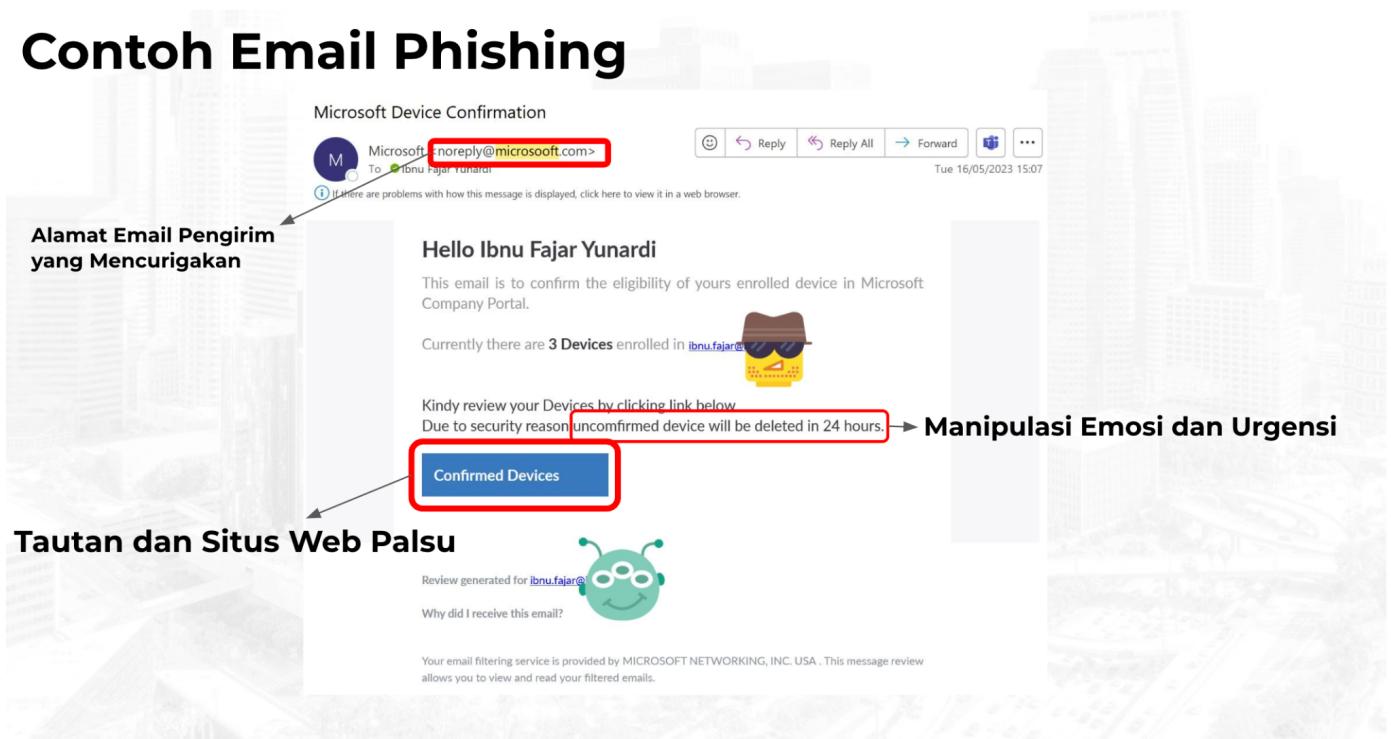
Jika menerima email yang meminta tindakan atau informasi penting, verifikasi dengan sumber yang sah melalui saluran komunikasi yang terpercaya, seperti situs web resmi atau nomor telepon resmi.

Aktifkan Autentikasi Dua Faktor (2FA)

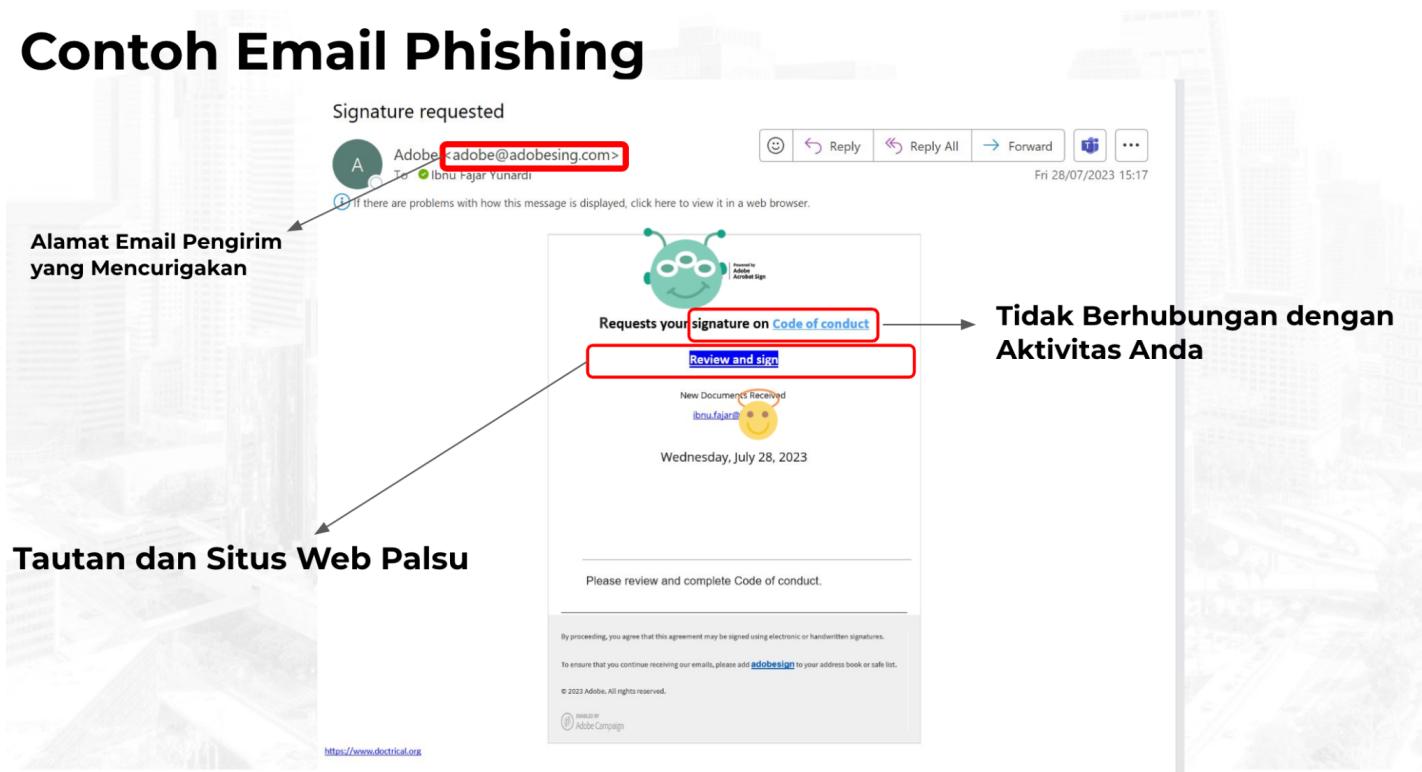
Aktifkan 2FA di akun online jika memungkinkan. Ini memberikan lapisan keamanan tambahan dengan memerlukan verifikasi melalui perangkat lain selain kata sandi. Jika merasa email mencurigakan, jangan memberi tanggapan atau mengikuti instruksi yang diberikan. Jika tidak yakin, lebih baik tidak mengambil risiko.

Contoh Email phishing

Contoh Email Phishing



Contoh Email Phishing



Tindakan Tanggapan Terhadap Phishing

Tindakan tanggapan yang tepat terhadap phishing sangat penting untuk melindungi diri dan mencegah kerugian lebih lanjut. Berikut adalah beberapa langkah yang harus diambil jika merasa telah menjadi korban serangan phishing:

Verifikasi Alamat Email Pengirim:

Selalu periksa alamat email pengirim dengan seksama sebelum merespons atau mengklik tautan. Pastikan alamat email cocok dengan yang diharapkan dari sumber yang sah.

Jangan Mengklik Tautan Langsung:

Jangan mengklik tautan di dalam email, terutama jika merasa mencurigai email tersebut. Alih-alih, arahkan kursor ke tautan untuk melihat URL yang sebenarnya sebelum mengkliknya.

Cek URL dengan Hati-hati:

Periksa URL yang ditampilkan ketika mengarahkan kursor ke tautan. Pastikan URL cocok dengan situs web yang seharusnya. Jika ada perbedaan, jangan mengkliknya.

Hati-hati dengan Lampiran:

Jangan membuka lampiran dari email yang tidak harapkan atau yang tampak mencurigakan. Lampiran berbahaya dapat mengandung malware atau ransomware.

Jangan Berikan Informasi Sensitif:

Tidak pernah memberikan informasi sensitif, seperti kata sandi, nomor kartu kredit, atau nomor jaminan sosial melalui email. Perusahaan sah umumnya tidak akan meminta informasi tersebut melalui email.

Verifikasi dengan Sumber yang Terpercaya:

Jika menerima email yang meminta tindakan atau informasi penting, verifikasi dengan sumber yang sah melalui saluran komunikasi yang terpercaya, seperti situs web resmi atau nomor telepon resmi.

Aktifkan Autentikasi Dua Faktor (2FA):

Aktifkan 2FA di akun online jika memungkinkan. Ini memberikan lapisan keamanan tambahan dengan memerlukan verifikasi melalui perangkat lain selain kata sandi.

