Klinik Digital

litnus.

WASPADA !

KEJAHATAN *PHISHING ATTACK!*

Devie Rahmawati | Mila Viendyasari | Giri Lumakto
Rienzy Kholifatur | Wiratri Anindhita | Rizki Ameliah
Syavia Bachna | Aisyah Adienda

KEJAHATAN *PHISHING ATTACK!*

Devie Rahmawati | Mila Viendyasari | Giri Lumakto
Rienzy Kholifatur | Wiratri Anindhita | Rizki Ameliah
Syavia Bachna | Aisyah Adienda

Penerbit litnus.

WASPADA KEJAHATAN PHISHING ATTACK!

Ditulis oleh:

Devie Rahmawati | Mila Viendyasari | Giri Lumakto
Rienzy Kholifatur | Wiratri Anindhita | Rizki Ameliah
Syavia Bachna | Aisyah Adienda

Dewan Pembina:

Prof. Dr. Drg. Indang Trihandini., M.Kes.
Prof. Dr. Rer. Nat. Rosari Saleh

Tim Riset:

Muhammad Ruslan Ramli | Youna A Bachtiar | Ballian Siregar

Diterbitkan, dicetak, dan didistribusikan oleh
PT. Literasi Nusantara Abadi Grup
Perumahan Puncak Joyo Agung Residence Kav. B11 Merjosari
Kecamatan Lowokwaru Kota Malang 65144
Telp: +6285887254603, +6285841411519
Email: literasinusantaraofficial@gmail.com
Web: www.penerbitlitnus.co.id
Anggota IKAPI No. 340/JTI/2022

Cetakan I, Mei 2024

Perancang sampul: Hasanuddin
Penata letak: Dicky Gea Nuansa

ISBN: 978-623-114-655-7

vi + 86 hlm. ; 14,8 x 21 cm.

KATA PENGANTAR

Segala Puji dan Syukur kami panjatkan selalu kepada Tuhan Yang Maha Esa atas Rahmat, Taufiq, dan Hidayah yang sudah diberikan sehingga kami bisa menyelesaikan modul panduan yang berjudul "Waspada Kejahatan *Phishing Attack*" dengan tepat waktu. Tujuan dari penulisan modul ini tidak lain adalah untuk membantu para masyarakat di dalam memahami seperti apa *Penipuan Phishing* yang ada di dunia digital, sehingga harapannya masyarakat bisa mengetahui tahapan apa saja yang harus dilakukan.

Modul ini juga akan memberikan informasi secara lengkap mengenai pengertian, macam, tujuan, dan banyak contoh dari Kejahatan *Phishing Attack*.

Kami juga sadar bahwa modul yang kami buat masih tidak belum bisa dikatakan sempurna. Maka dari itu, kami meminta dukungan dan masukan dari para pembaca, agar kedepannya kami bisa lebih baik lagi di dalam menulis sebuah modul.

Tim Penulis

Daftar Isi

PHISHING SEBAGAI KEJAHATAN DIGITAL

Source : https://money.kompas.com/read/2022/06/16/183024326/apa-itu-phising-definisi-cara-kerja-ciri-ciri-dan-cara-mencegahnya?page=all

Kejahatan Digital semakin marak dan sudah bukan menjadi rahasia lagi selama beberapa tahun terakhir ini. Masyarakat yang semakin bergantung dengan teknologi untuk mengerjakan pekerjaan atau berkomunikasi sehari-hari memakai ponsel yang selalu digenggam dimanapun dan kapanpun. Perlu kita ketahui bahwa semua kegiatan

ini menghasilkan sejumlah besar data dan informasi yang disimpan di komputer, ponsel, atau jenis jaringan komputer lainnya. Jika data dan informasi yang dimaksud tidak memiliki keamanan dan perlindungan yang memadai, maka akan rentan dalam kaitannya dengan curian data. Kejahatan digital meningkat setiap kali kegiatan ilegal yang melibatkan data atau informasi di komputer atau jaringan lain sedang dilakukan. Pada awalnya, kejahatan digital seperti ini sebagian besar dilakukan di sektor keuangan, tetapi sekarang telah diperluas untuk mencakup peran lain, seperti sistem informasi yang kita pakai sehari-hari sebagai masyarakat biasa.

Karena kenyataannya bahwa data tertentu dan lainnya dapat dikompromikan atau bocor dalam suatu organisasi oleh individu, komputer atau perangkat seluler juga dapat digunakan sebagai alat untuk melakukan penilaian keamanan, dan secara umum, tingkat kejahatan digital terus meningkat setelah munculnya Internet. Jaringan internet juga mengejar tujuan penting untuk meningkatkan tingkat perdamaian dunia. Tingginya biaya kejahatan digital dan kerusakan yang diakibatkannya, memanggil komunitas internasional dan pakar hukum dari beberapa negara untuk membuat undang-undang kejahatan digital dan memberlakukannya di dalam negara.

Ada beberapa kejahatan dalam digital yang perlu kita ketahui. Dalam modul ini, akan membahas tentang salah satu kejahatan digital, yakni Phishing. Phishing adalah bentuk kejahatan dunia maya yang paling umum yang melibatkan pencurian informasi pribadi dan data sensitif orang lain dengan mengirimi mereka pesan, email, atau komunikasi digital lainnya. Pelaku phishing sering menggunakan teknik seperti mengirim email phishing, dokumen berbahaya, atau pesan instan yang mencurigakan untuk menargetkan individu dan

mendapatkan informasi sensitif seperti kata sandi, nomor kartu kredit, dan detail keuangan lainnya.

Tujuan utama phishing adalah mencuri identitas target atau mendapatkan akses ilegal ke akun seseorang. Dengan informasi yang dimiliki pelaku phishing, pelaku dapat melakukan berbagai jenis penipuan, seperti pencurian identitas, pencucian uang, atau serangan terhadap komputer dan sistem jaringan. Phishing dapat memiliki dampak yang sangat serius bagi korban, seperti kerugian finansial, pencurian identitas, kehilangan data pribadi, atau hal-hal lainnya. Karena itu, penting bagi pengguna internet untuk waspada terhadap serangan phishing dan mengenali berbagai jenis tindakan keamanan yang dapat mereka ambil, seperti tidak mengklik tautan yang mencurigakan, memeriksa ulang validitas email dan pesan lainnya, dan menahan diri untuk tidak membocorkan informasi sensitif melalui saluran komunikasi yang tidak aman. Phishing juga memiliki beberapa teknik untuk mencuri identitas. Teknik tersebut akan dibahas lebih lanjut dalam modul ini.

A. KAJIAN PHISING

Istilah 'phishing' berasal dari kata 'fishing' yang diplesetkan. Namun jelas istilah ini tidak berbanding aktivitasnya dengan nelayan. Dengan kata lain phisher tidak memancing ikan. Phisher yang online akan lebih senang memancing informasi yang berharga. Secara definisi, phishing adalah upaya untuk mencuri data sensitif dengan menipu seseorang untuk memberikan kata sandi atau data kartu kredit, atau mengunduh virus komputer. Ini adalah kerugian ganda, karena korban kehilangan data dan uang mereka.

Secara prakteknya, aktivitas phishing adalah bentuk kejahatan siber yang bertujuan untuk menipu orang-orang agar mengungkapkan

informasi sensitif. Phishing dilakukan dengan mengirimkan email, telepon, atau pesan teks yang seolah-olah berasal dari lembaga resmi. Para phisher akan memancing individu agar memberikan data pribadi seperti informasi identitas, rincian perbankan dan kartu kredit, dan kata sandi. Informasi atau akses yang diperoleh kemudian dapat digunakan untuk mencuri uang, mengunduh dan menginstal malware. Mereka juga akan melakukan spear phishing terhadap orang lain di dalam organisasi target.

Phishing menjadi salah satu jenis kejahatan siber berupa pencurian data, yang bisa menimbulkan kerugian serius bagi korbannya. Pelaku phishing biasanya beraksi dengan berpura-pura menjadi perusahaan atau lembaga berwenang, kemudian mengirim e-mail berisi tautan website atau situs tertentu kepada korban. Hal itu dilakukan supaya korban terkecoh dan mau memasukkan informasi pentingnya ke situs phishing, seperti nama akun (username) aplikasi perbankan, kata sandi (password), nomor pin, dan sebagainya. Setelah datanya masuk, pelaku pun bisa leluasa menggasak isi rekening korban atau melakukan aksi kejahatan lainnya.

Phishing juga bisa dilakukan dengan modus social engineering. Modus ini dilakukan dengan pelaku menghubungi korban melalui telepon, chat, sosial media, dan platform digital lain, lalu mengarahkan korban untuk membuka situs tertentu dengan tujuan pencurian data serupa. Para pelaku memperhatikan perilaku atau kebiasaan calon korban untuk menemukan kelemahan mereka. Ada pula phishing yang bertujuan menanamkan malware atau virus ke perangkat digital korban, supaya pelaku bisa mencuri data korban secara otomatis (Chaudry, 2014).

Serangan phishing biasanya dikirim melalui email, tetapi mereka juga dapat menggunakan saluran lain seperti panggilan telepon,

pesan teks, chat, atau tautan situs web jahat. Para phisher sering menyamar sebagai entitas terpercaya seperti bank, layanan online, atau rekan kerja untuk menarik korban untuk mengklik tautan atau lampiran jahat, atau memberikan informasi pribadi atau keuangan. Para phisher kemudian menggunakan informasi ini untuk mengakses akun korban, mencuri identitas mereka, atau memeras uang dari mereka.

Adapun cara kerja phishing yang perlu diketahui. Meskipun peringatan berulang dan edukasi terkait cara menghindari penipuan phishing, banyak orang dan organisasi masih terus menjadi korban dari kejahatan siber macam ini. Berikut adalah tiga alasan utama mengapa tindak kejahatan siber phishing tetap menjadi teknik umum dan efektif untuk penjahat dunia maya.

1. Pesatnya pertumbuhan jejaring sosial telah membuatnya sangat nyaman untuk mendapatkan informasi spesifik tentang korban yang dipilih. Para pelaku kejahatan phishing atau phisher sering mengumpulkan data yang relevan secara manual dengan menggunakan perangkat lunak yang mengakses API (Application Programming Interface) yang disediakan oleh sebagian besar jejaring sosial.
2. Pola pelanggaran data: Ada pola pelanggaran data yang berkelanjutan di mana email dan data identifikasi pribadi telah dicuri. Cobalah untuk menghapus jejak mereka setelah mendapatkan apa yang mereka inginkan. Intinya: Sejumlah besar informasi curian tersedia di luar sana untuk dieksploitasi.
3. Aktivitas ini juga mengeksploitasi ketakutan korban: Teknik yang umum adalah menakut-nakuti korban dengan mengirimi mereka email yang mengklaim rekening mereka terancam dan perlu diperbaiki dengan mengklik tautan. Jika pengguna

mengikuti tautan, mereka dibawa ke situs web palsu yang meniru situs web bank dan meminta mereka untuk memasukkan nama pengguna dan kata sandi mereka. Setelah mereka mengirimkan formulir, semua data mereka dikirim ke server penyerang. Pengguna yang memiliki banyak uang di rekening bank mereka mungkin panik ketika mereka melihat email ini dan beberapa dari mereka mungkin mengklik tautan untuk mencegah akun mereka disusupi (Chanti, S., & Chithralekha, 2022).

Secara historis, phishing juga telah terekam di dunia digital. Sebagai salah satu bentuk serangan siber, phishing dapat dilacak kembali ke pertengahan 1990-an, ketika peretas mulai menggunakan teknik yang disebut spoofing untuk mencuri kata sandi pengguna America On-line (AOL). Spoofing dilakukan dengan membuat halaman login AOL palsu dan mengirimkannya ke pengguna yang tidak curiga melalui email atau pesan instan. Namun secara spesifik kemudian istilah "phishing" diciptakan pada tahun 1996 oleh peretas yang menggunakan metode ini untuk *fishing* atau "memancing" kata sandi pengguna yang lengah (Gillin, 2020).

Seiring dengan semakin populer dan beragamnya internet, sindikat penipuan dunia online juga menyesuaikan taktik dan sasaran mereka. Pada tahun 1998, mereka mulai mengeksploitasi forum dan grup diskusi online, yang merupakan platform online dimana pengguna dapat memposting dan mendiskusikan berbagai topik. Para penipu online akan membuat postingan atau balasan palsu yang berisi tautan atau lampiran berbahaya. Sehingga tautan ini akan menarik pengguna untuk mengkliknya. Tautan atau lampiran ini akan mengarahkan pengguna ke situs web palsu atau menginstal perangkat lunak jahat di perangkat mereka.

Contoh lain asal muasal phishing juga terjadi pada tahun 1999, seorang peretas memposting pesan di grup diskusi Microsoft yang mengklaim memiliki perbaikan untuk celah keamanan di Internet Explorer. Pesan tersebut berisi tautan ke situs web yang tampak seperti situs resmi Microsoft, tetapi sebenarnya dikendalikan oleh peretas. Pengguna yang mengklik tautan dan mengunduh perbaikan tersebut terinfeksi dengan kuda Troya yang memberi peretas akses ke komputer mereka.

Pada pergantian milenium, para phisher sudah memiliki akses, alat, dan teknik yang lebih canggih, seperti pengirim massal, yang memungkinkan mereka mengirim email phishing ke ribuan penerima sekaligus. Pengirim massal juga memungkinkan para penipu phishing untuk menyesuaikan email mereka berdasarkan profil dan preferensi penerima, sehingga membuat mereka lebih meyakinkan dan menarik. Email phishing sering meniru gaya dan format email resmi dari organisasi atau individu yang terkenal, seperti bank, situs e-commerce, lembaga pemerintah, atau selebriti. Konten email ini biasanya berisi rasa mendesak atau tawaran menarik. Email ini juga meminta pengguna untuk mengklik tautan atau membuka lampiran untuk memverifikasi identitas mereka, memperbarui akun mereka, mengklaim hadiah, atau mengakses layanan.

Sebagai contoh, pada tahun 2003, jutaan pengguna menerima email yang tampaknya berasal dari PayPal, meminta mereka untuk memperbarui informasi akun mereka karena adanya pelanggaran keamanan. Email tersebut berisi tautan ke situs web PayPal palsu yang meminta pengguna untuk memasukkan rincian pribadi dan keuangan mereka. Pengguna yang tertipu oleh penipuan ini kehilangan akun dan uang mereka. Salah satu korban penipuan tersebut mengatakan bahwa ia pikir email itu asli karena logo dan tata letaknya sama

dengan PayPal. Ia tidak menyadari bahwa tautannya mengarah ke situs web palsu sampai saya melihat bahwa uangnya telah dicuri dari rekeningnya.

Sehingga sampai dengan tahun 2020, phishing adalah jenis kejahatan siber yang paling umum menurut dengan Pusat Pengaduan Kejahatan Internet FBI. Mereka melaporkan lebih banyak insiden phishing daripada jenis kejahatan komputer lainnya. Motivasi di balik phishing bermacam-macam, dengan target umum meliputi lembaga keuangan, penyedia email dan produktivitas cloud, dan layanan streaming. Informasi atau akses yang dicuri dapat digunakan untuk hal-hal berikut:

1. Mencuri atau menangkap kredensial perbankan. Dengan cara ini, penyerang dapat mengakses rekening korban dan melakukan transaksi ilegal seperti transfer uang atau pembelian barang.
2. Mengumpulkan informasi pribadi. Informasi ini dapat digunakan untuk melakukan pencurian identitas, penipuan kartu kredit, atau pemerasan.
3. Menginfeksi komputer korban dengan malware. Malware adalah perangkat lunak berbahaya yang dapat merusak sistem, mencuri data, atau mengunci file korban sampai mereka membayar tebusan (ransomware).
4. Mencuri rahasia dagang dan dokumen rahasia. Phishing dapat digunakan untuk menargetkan organisasi bisnis, pemerintah, atau militer yang memiliki informasi penting yang dapat dijual atau disalahgunakan oleh penyerang.
5. Mendapatkan ketenaran. Beberapa penyerang phishing mungkin termotivasi oleh keinginan untuk mendapatkan pengakuan atau pujian dari komunitas peretas.

6. Mengeksploitasi bug keamanan. Phishing dapat digunakan untuk menemukan dan memanfaatkan celah keamanan di situs web atau aplikasi yang rentan terhadap serangan.

Phishing menjadi salah satu bentuk kejahatan siber yang luas dan terus berkembang. Dampaknya pun mempengaruhi individu dan bisnis. Menurut penelitian Tessian Defender di tahun 2021 menunjukkan hasil mengkhawatirkan. Antara Juli 2020 dan Juli 2021, Tessian Defender memeriksa hampir 4 miliar email dan mengidentifikasi hampir 2 juta sebagai kemungkinan berbahaya, menunjukkan peniruan identitas, rekayasa sosial, atau niat jahat. Sedang karyawan sebuah perusahaan secara global akan menerima rata-rata 14 email jahat per tahun. Penelitian Symantec menunjukkan bahwa sepanjang tahun 2020 ada 1 dari setiap 4.200 email adalah email phishing. Phishing juga merupakan penyebab paling umum dari pelanggaran data, menyumbang 90% dari pelanggaran data menurut Cisco (Tessian Defender.com, 2021).

Setiap kali para phisher menyerang dengan teknik yang berbeda untuk menipu pengguna internet agar mencuri kredensial pribadi mereka seperti detail rekening bank, e-banking, akun media sosial, akun email, dll. Jenis pharming yang merupakan bentuk phishing yang lebih canggih yaitu "phishing tanpa umpan menyerang mengirim email palsu dengan hyperlink tertanam ke pengguna individu. Dengan demikian pengguna dialihkan ke situs palsu yang secara menipu mencuri kredensial pengguna. Namun, dalam pharming, penyerang mencoba mengarahkan pengguna ke situs palsu yang sangat mirip dengan situs asli dengan meracuni sistem nama domain (DNS). Sehingga menurut laporan Anti-Phishing Work Group (APWG) kuartal ke-2 tahun 2021, hanya pada bulan Juni 2021 saja, jumlah serangan phishing di Indonesia mencapai 222.127 kasus. Tahun 2022

adalah tahun rekor untuk phishing. APWG menemukan ada lebih dari 4,7 juta serangan sepanjang tahun 2022 saja. Sejak awal 2019, jumlah serangan phishing sudah meningkat sekitar 150% per tahun menurut laporan Phishing Activity Trends Report 4th Quarter 2022 (APWG, 2021).

Indonesia dalam laporan Surfshark menempati posisi ke-8 dan masuk dalam jajaran 10 besar negara dengan jumlah kasus kebocoran data tertinggi di internet secara global, termasuk dari hasil kejahatan phishing. Menurut laporan dari perusahaan keamanan tersebut, terdapat sekitar 820 ribu kasus pembobolan yang tercatat di tanah air sepanjang periode kuartal II/2022 (Goodstats.id, 2023).

Menurut organisasi internasional APWG, tren kejahatan online jenis ini terus meningkat dari tahun ke tahun. APWG mengukur tren serangan phishing dari banyaknya jumlah situs phishing unik yang dikirimkan melalui e-mail secara global. Datanya berasal dari laporan mitra-mitra riset APWG di berbagai negara, serta dari aduan publik yang dilaporkan langsung ke situs APWG.

Menurut laporannya, APWG menemukan jumlah serangan phishing pada tahun 2022 naik jauh dibanding tahun-tahun sebelumnya. Sepanjang 2019, jumlah serangan yang dilaporkan masih di bawah 100 ribu situs phishing unik per bulan. Kemudian pada 2020-2021 jumlahnya mencapai kisaran 200 ribu situs per bulan, dan melonjak lagi ke kisaran 300 ribu-400 ribu situs per bulan hingga mencapai rekor tertinggi pada Desember 2022.

Phishing adalah salah satu metode penipuan online yang paling umum dan berbahaya pada tahap personal. Menurut laporan Data Breach Investigations Report di tahun 2019 oleh Verizon di Amerika Serikat, phishing merupakan penyebab tertinggi kebocoran data (32%). Phishing bertujuan untuk mencuri data pribadi atau keuangan

korban dengan cara mengirimkan pesan atau mengarahkan korban ke situs web palsu yang meniru situs resmi. Dampak dari phishing bisa sangat merugikan bagi korban, baik secara finansial maupun psikologis (Verizon, 2019).

Di Indonesia sendiri phishing juga sering terjadi. Karena serangan phishing tidak hanya terjadi di negara-negara maju, tetapi juga di negara-negara berkembang seperti Indonesia. Menurut Indonesia Anti-Phishing Data Exchange (IDADX), total pengaduan serangan phishing di Indonesia mengalami peningkatan signifikan. Tercatat, IDADX menerima sebanyak 26.675 laporan serangan phishing pada periode kuartal I di tahun 2023.

Serangan phishing paling banyak terjadi di bulan Februari dengan jumlah aduan sebanyak 15.050 kasus. Sementara, jumlah di bulan Januari hanya sekitar 7.665 kasus dan di bulan Maret sebanyak 3.960 kasus. IDADX menyebut, terdapat beberapa SLD (Second Level Domain) yang menjadi target serangan phishing terbanyak sepanjang Q1 di tahun 2023, yakni id, biz.id, dan my.id (Databoks.com, 2023).

Menurut laporan dari Microsoft Indonesia tahun 2019, salah satu faktor yang memicu meningkatnya serangan phishing adalah pandemi COVID-19 yang membuat banyak orang bergantung pada layanan digital untuk berbagai keperluan. Sejak mulainya wabah, data tim Microsoft Intelligence Protection menunjukkan bahwa setiap negara di dunia telah melihat setidaknya satu serangan bertema COVID-19, dan volume serangan yang berhasil di negara-negara yang terkena wabah tampaknya naik, karena meningkatnya ketakutan dan keinginan informasi terkini. Dari jutaan pesan phishing yang ditargetkan secara global setiap harinya, sekitar 60.000 diantaranya bertema COVID-19, dengan lampiran berbahaya atau URL (alamat website) jahat (Microsoft.id, 2019).

Sehingga dari banyak laporan berbagai lembaga internasional dan nasional, mereka merekomendasikan langkah-langkah untuk mencegah atau mengurangi dampak serangan phishing meliputi undang-undang, edukasi pengguna, kesadaran publik, dan langkah-langkah keamanan teknis. Sehingga pentingnya kesadaran phishing telah meningkat baik di lingkungan pribadi maupun profesional, dengan serangan phishing. Dan perlu kita pahami juga beberapa dampak yang dilaporkan dari korban phishing antara lain:

Kerugian finansial. Korban phishing bisa kehilangan uang secara langsung jika mereka memberikan informasi rekening bank atau kartu kredit kepada penipu. Penipu bisa menguras saldo atau melakukan transaksi ilegal dengan menggunakan data tersebut. Selain itu, korban juga bisa kehilangan uang secara tidak langsung jika data mereka dijual kepada pihak lain yang bisa memanfaatkannya untuk melakukan kejahatan lainnya, seperti pencurian identitas atau pemerasan.

Menurut Federal Trade Commission (FTC) Amerika Serikat, kerugian akibat penipuan online di media sosial mencapai 11 triliun rupiah pada tahun 2021. Sedang menurut laporan dari FBI, pada tahun 2020, phishing merupakan jenis kejahatan siber yang paling banyak dilaporkan di Amerika Serikat, dengan total kerugian mencapai lebih dari 4,2 miliar USD. Laporan lain dari Proofpoint sebuah perusahaan keamanan siber global menunjukkan bahwa pada kuartal pertama tahun 2021, ada peningkatan 25% dalam jumlah serangan phishing yang ditujukan kepada sektor kesehatan, keuangan, dan sektor ritel.

Kerusakan reputasi. Korban phishing juga bisa mengalami kerusakan reputasi jika data mereka digunakan untuk melakukan aktivitas yang merugikan atau melanggar hukum. Misalnya, para phisher bisa menggunakan akun email atau media sosial korban untuk

mengirimkan spam, malware, atau konten tidak pantas kepada orang lain. Hal ini bisa merusak citra dan kepercayaan korban di mata orang lain, terutama jika mereka adalah pelaku bisnis atau pejabat publik.

Phishing terbukti telah dapat menyebabkan kerusakan reputasi yang besar bagi seseorang atau institusi yang menjadi targetnya, karena informasi yang dicuri dapat digunakan untuk tujuan kejahatan, seperti penipuan, pencurian identitas, atau penyalahgunaan akun. Beberapa contoh peristiwa phishing yang merusak reputasi adalah sebagai berikut:

1. Pada tahun 2020, Kementerian Keuangan di Amerika Serikat mengeluarkan klarifikasi bahwa email yang mengatasnamakan instansinya dan meminta data pribadi adalah email phishing yang tidak resmi. Email tersebut dapat merusak citra Kementerian Keuangan sebagai lembaga pemerintah yang bertanggung jawab atas keuangan negara (Carnegie Endowment.com, 2021).
2. Pada tahun 2021, beberapa perusahaan besar mengalami pelanggaran data akibat phishing yang menargetkan karyawan mereka. Pelanggaran data ini dapat mengancam keamanan informasi pelanggan, mitra, dan pemasok perusahaan, serta menimbulkan kerugian finansial dan hukum. Pelanggaran data juga dapat menurunkan kepercayaan publik terhadap perusahaan tersebut.
3. Pada tahun 2022, seorang artis terkenal menjadi korban phishing yang menyamar sebagai platform media sosial. Akun media sosialnya diretas dan digunakan untuk menyebarkan konten negatif dan provokatif yang merendahkan nama baiknya. Akibatnya, artis tersebut mendapat banyak kritik dan hujatan dari netizen, serta kehilangan sebagian penggemarnya (Wazirx.com, 2020).

Stres dan trauma. Korban phishing bisa mengalami stres dan trauma akibat pengalaman yang tidak menyenangkan dan meresahkan. Para korban bisa merasa takut, marah, bersalah, malu, atau depresi karena menjadi korban penipuan. Mereka juga bisa merasa tidak aman dan khawatir tentang data dan privasi mereka di dunia maya. Stres dan trauma ini bisa berdampak negatif pada kesehatan mental dan fisik korban. Beberapa dampak psikologis yang bisa ditimbulkan oleh phishing adalah:

1. Stres. Korban phishing bisa merasa stres karena khawatir data pribadi mereka disalahgunakan oleh pelaku, atau karena mendapat tekanan dari pihak-pihak yang terkait dengan data yang dicuri, seperti bank, perusahaan, atau instansi pemerintah.
2. Trauma. Korban phishing bisa mengalami trauma yang membuat mereka takut atau ragu untuk menggunakan layanan online lagi, seperti berbelanja online, bertransaksi online, atau berkomunikasi online.
3. Depresi. Korban phishing bisa mengalami depresi karena merasa bersalah, malu, atau rendah diri akibat menjadi korban penipuan online. Depresi juga bisa disebabkan oleh kerugian finansial yang besar atau hilangnya kepercayaan dari orang-orang di sekitar mereka.
4. Kecemasan. Korban phishing bisa mengalami kecemasan karena tidak tahu bagaimana cara mengatasi masalah yang ditimbulkan oleh phishing, atau karena khawatir akan menjadi korban phishing lagi di masa depan (Liputan6.com, 2020).

Untuk menghindari dampak psikologis tersebut, korban phishing perlu melakukan beberapa hal, seperti:

1. Melaporkan kasus phishing kepada pihak yang berwenang, seperti bank, perusahaan, instansi pemerintah, atau polisi cyber crime.
2. Mengganti password atau data akses yang dicuri oleh pelaku phishing dengan segera.
3. Menjaga kesehatan mental dengan mencari dukungan dari keluarga, teman, atau profesional kesehatan mental jika diperlukan.
4. Meningkatkan kewaspadaan dan pengetahuan tentang cara mencegah dan mengenali phishing.

Untuk menghindari dampak-dampak tersebut, korban phishing perlu segera melaporkan kejadian tersebut kepada pihak yang berwenang, seperti bank, penyedia layanan internet, atau polisi. Mereka juga perlu mengubah kata sandi dan kredensial yang terkait dengan data yang dicuri, serta memeriksa laporan keuangan dan kredit mereka secara berkala. Selain itu, korban juga perlu mendapatkan dukungan dari keluarga, teman, atau profesional untuk mengatasi dampak psikologis dari phishing.

Setiap hari, email, tautan, dan pesan DM phishing digunakan untuk mencuri uang dan informasi sensitif dari bisnis. Sementara penipuan apa pun bisa berbahaya, beberapa jauh lebih besar daripada yang lain dalam hal jumlah kerugian yang mereka timbulkan pada korban mereka. Beberapa skema phishing telah dikaitkan dengan pencurian puluhan juta dolar. Yang lain telah digunakan untuk membocorkan dokumen militer yang sensitif atau untuk mendisrupsi e-banking. Dengan meningkatnya serangan Untuk menghindari

serangan phishing secara umum, ada beberapa langkah yang bisa dilakukan, antara lain:

1. Selalu waspada terhadap e-mail atau pesan yang mencurigakan, terutama yang meminta informasi pribadi atau keuangan.
2. Jangan pernah membuka lampiran atau mengklik tautan dari sumber yang tidak dikenal atau tidak terpercaya.
3. Periksa alamat e-mail atau situs web dengan teliti, dan cari tanda-tanda penipuan, seperti kesalahan ejaan, logo yang tidak sesuai, atau domain yang aneh.
4. Gunakan perangkat lunak antivirus dan firewall yang terbaru dan terpercaya untuk melindungi perangkat digital dari malware atau virus.
5. Ubah kata sandi secara berkala menggunakan kata sandi yang kuat dan unik untuk setiap akun online.
6. Laporkan segala bentuk serangan phishing ke pihak berwenang, seperti IDADX, APWG, atau lembaga lain yang relevan.

Referensi:

APWG.com. (2021). Phishing Activity Trends Reports. https://apwg.org/trendsreports/

vDataboks.co.id. (2023). Tren Serangan Phishing Terus Meningkat Capai Rekor Tertinggi Pada 2022. https://databoks.katadata.co.id/datapublish/2023/05/17/tren-serangan-phishing-terus-meningkat-capai-rekor-tertinggi-pada-2022

Carnegie Endowmnet. (2020). Protecting Financial Stability https://carnegieendowment.org/specialprojects/protectingfinancialstability/timeline

Chanti, S., & Chithralekha, T. (2022). A literature review on classification of phishing attacks. International Journal of Advanced Technology and Engineering Exploration, 9(89), 446.

Chaudhary, G. K. (2014). Development review on phishing: a computer security threat. International journal of advance research in computer science and management studies, 2(8), 55-64.

Ekonomy Okezone.com. (2021). Peristiwa ini Bikin Reputasi Perusahaan Rusak. https://economy.okezone.com/read/2021/03/25/455/2383886/5-peristiwa-ini-bikin-reputasi-perusahaan-rusak

Gillin, Paul. (2020). The History of Phishign. https://www.verizon.com/business/resources/articles/s/the-history-of-phishing

Glints.com. Phishing. https://glints.com/id/lowongan/phishing/

Goodstats.id. (2022). Serangan Phishing di Indonesia Terus Meningkat, ini Statistiknya. https://goodstats.id/article/serangan-phishing-di-indonesia-terus-meningkat-ini-statistiknya-U8VdY

Haloedukasi.com. Phishing. https://haloedukasi.com/phising

Kompas.com. (2021). Apa Saja Dampak Psikologis Akibat Terjerat Pinjaman Online https://www.kompas.com/sains/read/2021/08/23/120200623/apa-saja-dampak-psikologis-akibat-terjerat-pinjaman-online-ini

Liputan6.com. (2020). Tak Hanya Phishing, ini 9 Metode Serangan Siber yang Perlu Diketahui. https://www.liputan6.com/cek-fakta/read/5280986/tak-hanya-phising-berikut-ini-9-metode-serangan-siber-yang-perlu-diketahui

Microsoft.id. (2020). Tingkat Kasus Malware di Indonesia Tertinggi di Asia Pasifik. https://news.microsoft.com/id-id/2020/06/26/tingkat-kasus-malware-di-indonesia-tertinggi-di-asia-pasifik-laporan-microsoft-security-endpoint-threat-2019

Niagahoster.co.id. Mengatasi Phishing. https://www.niagahoster.co.id/blog/mengatasi-phishing/

Rumahwweb.com. Phishing Adalah. https://www.rumahweb.com/journal/phishing-adalah/

Tessian Defender. (2021). Why Organizations Need New Methods to Combat New Tricks https://www.tessian.com/research/spear-phishing-threat-landscape/

Verizon.com. (2019). DBIR: Results and Analysis. https://www.verizon.com/business/resources/reports/dbir/2019/results-and-analysis/

Wazirx.com. (2021). https://wazirx.com/news/beeple-an-nft-artist-got-his-twitter-account-hacked-in-a-phishing-scam/

CARA KERJA PHISHING

Pelaku phishing akan menggunakan berbagai metode untuk mendapatkan informasi rahasia. Di bawah ini adalah beberapa tugas yang dilakukan oleh pengguna phising:

1. Email Palsu: Pelaku phishing akan mengirim email yang tampaknya berasal dari organisasi atau bisnis yang sah. Email yang disebutkan di atas seringkali menyertakan rasa keperluan, kepentingan atau permintaan penerima untuk mengirim pesan sesegera mungkin. Dalam email yang disebutkan di atas, penerima akan diberikan opsi untuk mengklik tautan yang akan membawa mereka ke situs web berbahaya atau memasukkan informasi pribadi seperti kata sandi, nomor kartu kredit, atau informasi keuangan lainnya. Setelah korban memberikan informasi yang disebutkan di atas, orang yang terlibat dalam phishing dapat menggunakannya untuk tujuan yang dimaksudkan.
2. Situs Web Palsu: Pelaku phishing dapat membuat situs yang mereplikasi situs web resmi perusahaan terkenal, seperti bank, penyedia email, atau platform media sosial. Mereka menggunakan teknik desain dan konstruksi serupa untuk menghilangkan korban. Ketika korban phishing mengunjungi

situs web berbahaya dan memasukkan informasi pribadi, maka hal tersebut menjadi jebakan dan digunakan untuk tujuan jahat.

3. Pesan Teks dan Pesan Instan (SMS): Pengguna phishing juga dapat menggunakan pesan teks atau pesan instan untuk mengelabui perampok agar memberi mereka informasi pribadi. Artikel di atas sering berisi tautan yang merujuk ke situs web yang rentan atau meminta izin dari polisi untuk menggunakan informasi sensitif. Untuk mendapatkan kepercayaan dari angkatan bersenjata, tersangka phishing dapat menyamar sebagai bank, penyedia layanan, atau kenalan yang akrab.
4. Rekayasa Sosial: Pelaku phishing sering menggunakan teknik ini untuk memanipulasi target (korban) agar memberikan informasi rahasia. Mereka dapat mencari informasi tentang korban dari masyarakat umum, seperti media sosial, dan kemudian menggunakan informasi itu untuk menyaring komentar yang tampak mencurigakan atau yang mereka yakini sebagai orang yang memiliki wewenang untuk membocorkan informasi sensitif.
5. Memanipulasi korban: Pelaku phishing sering mencoba memanipulasi emosi target untuk mendapatkan respons yang lebih cepat dan tidak menentu. Misalnya, pesan dapat menyembunyikan aktivasi akun atau menawarkan informasi yang sangat aman lalu kemudian meyakinkan korban untuk memberikan informasinya.

Pelaku phishing terus berinovasi dan menggunakan metode yang semakin berbahaya dalam upaya mereka memperoleh data kriminal. Karena itu, penting bagi pengguna internet untuk selalu waspada dan berhati-hati saat berhadapan dengan email, pesan, atau situs web yang menyertakan kode berbahaya.

Phishing telah menjadi bentuk kejahatan digital yang serius karena beberapa hal ini :

1. Kelemahan dalam pendeteksian: Salah satu kelemahannya adalah bahwa email phishing seringkali sangat sulit dibedakan dari komunikasi yangasli. Pelaku sering melakukan canggih teknik untuk menyesuaikan pesan dengan konteks yang tepat dan menyamarkan identitas palsu mereka.
2. Skala dan jangkauan yang luas: Serangan phishing dapat diluncurkan kepada sejumlah besar orang dalam satu hari. Mungkin jika hanya ada sejumlah kecil informasi yang bergerak, pengguna dapat memperoleh akses ke beberapa akun yang berisi informasi sensitif.
3. Kerugian finansial dan kerusakan reputasi: Jika informasi pribadi atau dana seseorang ditransfer ke akun yang salah, hal tersebut dapat membuka jalan kerugian finansial yang signifikan bagi korban. Selain itu, dapat merusak reputasi perusahaan jika menjadi target serangan phishing dan kebocoran data pelanggan.
4. Taktik phishing untuk serangan jarak jauh: Informasi yang diperoleh melalui serangan phishing dapat digunakan untuk melakukan serangan jarak jauh, seperti akses ilegal ke sistem.
5. Peringatan malware: Dalam beberapa kasus, pesan phishing dapat mengandung lampiran berbahaya atau tautan yang mengarahkan korban ke situs web yang menginfeksi perangkat dengan malware. Malware ini merupakan perangkat lunak dalam komputer yang dapat digunakan untuk mencuri informasi, mengontrol perangkat korban, atau meluncurkan serangan lanjutan.

6. Menargetkan individu dan organisasi: Pelaku / penyerang phishing ini sering melakukan penelitian pada individu atau organisasi yang ditargetkan untuk mengembangkan serangan phishing nya yang sangat mengkhawatirkan. Mereka dapat membuat pesan yang lebih realistis dan meningkatkan kemungkinan serangan dengan mengumpulkan informasi tentang potensi korban, seperti nama, tempat kerja, atau aktivitas internet.
7. Memanfaatkan teknik penalaran sosial: Pelaku phishing sering menggunakan teknik penalaran sosial di mana korban diminta untuk memanipulasi emosi, perasaan ingin tahu, atau kepercayaan mereka pada penipu. Mereka mungkin menggunakan tekanan waktu, ancaman, janji keuntungan besar untuk mempengaruhi korban agar melakukan tindakan yang diminta.
8. Kemajuan pada Teknik phishing: Penyerang terus menggunakan teknik phishing mereka sendiri untuk menggagalkan pendeteksian dan meningkatkan kekuatan serangan. Mereka dapat menggunakan sistem kekebalan dalam kerentanan sistem keamanan, menyesuaikan bobot mereka sendiri dengan fenomena viral saat ini, atau menggunakan metode baru untuk mencuri informasi sensitif.

Phishing adalah risiko keamanan yang serius karena dapat mengakibatkan kerugian finansial, kehilangan data, pencurian identitas, dan bahkan pengungkapan informasi pribadi. Untuk melindungi diri anda dari serangan phishing, penting untuk selalu waspada terhadap ancaman, memverifikasi informasi sensitif yang mengandung data pribadi, dan menggunakan teknik pencegahan

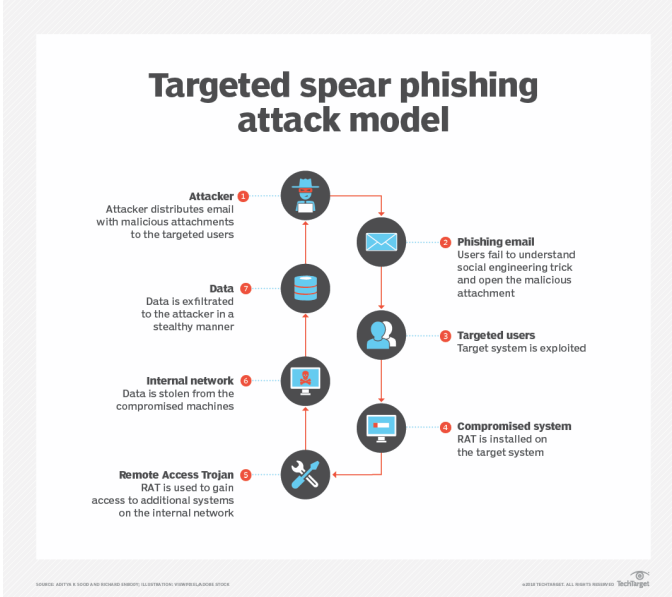
phishing terpercaya seperti perangkat lunak *anti-phishing* dan pelatihan phishing yang mudah digunakan.

A. GAMBARAN UMUM TEKNIK DAN METODE SERANGAN PHISHING

Pelaku phishing adalah seseorang yang menyamar sebagai orang lain untuk mendapatkan informasi akun sensitif atau informasi login lainnya secara online. Setiap jenis phishing dirancang untuk menghasilkan uang. Kenyataannya saat ini begitu banyak orang melakukan bisnis online. Karena itu, phishing telah menjadi ancaman keamanan siber yang paling umum, bersama dengan serangan penolakan layanan terdistribusi, kebocoran data, dan berbagai jenis malware.

Mengetahui beberapa jenis teknik phishing akan membantu anda untuk melindungi diri sendiri, organisasi, dan orang-orang di lingkungan anda. Ada 19 gambaran umum teknik dan metode dalam serangan phishing, yakni:

1. Spear Phishing



Spear phishing adalah jenis serangan phishing yang sangat menyesuaikan dan menargetkan orang-orang tertentu. Dalam *spear phishing*, penyerang melakukan pengintaian pada target, baik individu atau organisasi, untuk memberikan informasi yang tampak asli dan kredibel. Serangan seperti ini biasanya ditujukan kepada mereka yang memiliki akses ke informasi penting atau yang memiliki pengetahuan orang dalam tentang organisasi tertentu.

Berbeda dengan phishing umum yang lebih canggih, spear phishing menargetkan target tertentu dan menggunakan informasi pribadi yang dikumpulkan sebelumnya untuk meningkatkan kemungkinan serangan yang berhasil. Penyerang dapat mencari informasi tentang target yang dituju dari sumber

publik seperti media sosial, situs web perusahaan, atau iklan berbasis online.

Berikut ini adalah langkah-langkah umum yang digunakan dalam skema spear phishing:

a. Pemetaan target: Penyerang mengidentifikasi target potensial dan mengambil tindakan untuk mengumpulkan informasi tentang mereka, seperti melalui pertemuan, peran anda dalam organisasi, percakapan, dan *history* internet.
b. Penyesuaian pesan: Berdasarkan informasi yang diperoleh, penyerang membuat pesan yang dipersonalisasi, meniru pengirim yang dapat dipercaya, atau entitas yang dikenal target. Pesan ini secara konsisten keluar sebagai seseorang yang sangat samar anda kenal dan seperti sedang berkomunikasi asli.
c. Upaya Manipulasi: Pesan yang telah dipersonalisasi dimaksudkan untuk mengelola target agar penyerang dapat melakukan tindakan yang mereka inginkan, seperti mengklik tautan berbahaya, membocorkan informasi pribadi, atau menginstal malware.
d. Pengiriman pesan: Penyerangan *spear phishing* dapat dikirim melalui email, pesan instan, media sosial, atau bahkan pesan tertulis. Penyerang dapat meningkatkan kemungkinan keberhasilan dalam suatu situasi dengan memanfaatkan berbagai teknik manipulasi psikologis.
e. Eksploitasi dan kebocoran informasi: Jika target rentan dan terlibat dalam tindakan yang dilarang oleh penyerang, informasi pribadi yang sensitif dapat diungkapkan secara

penjualan ke orang lain, atau tindakan berbahaya lainnya dapat terjadi.

f. Untuk melindungi diri anda dari *Spear Phishing*, ada beberapa hal yang mungkin harus anda lakukan, yaitu :

g. Waspadai Pesan Mencurigakan: Perhatikan detail seperti pengejaan kesalahan, alamat email yang mencurigakan, atau permintaan informasi pribadi yang tidak biasa.

h. Verifikasi pengirim: Periksa alamat email pengirim, konfirmasi melalui saluran komunikasi yang berbeda, atau hubungi organisasi terkait secara informasi yang informal.

i. Pendidikan dan akademisi: Pertimbangkan untuk belajar tentang *spear phishing* dan berbagi pengetahuan tentang taktik lain yang digunakan oleh anggota organisasi lainnya.

j. Pertahankan kerahasiaan informasi pribadi: Hindari mengirim informasi sensitif melalui komunikasi yang tidak dapat diandalkan atau tidak diverifikasi.

k. Gunakan solusi keamanan yang kuat: Tempel perangkat lunak pengamanan.

2. Email Phishing

Source: https://www.msvu.ca/wp-content/uploads/2017/10/account-termination-phish-2022-09-29_12-05-23.png

Email phishing adalah jenis penipuan ketika korban setuju untuk memberikan informasi sensitif atau melakukan kegiatan ilegal menggunakan akun email yang disusupi atau diretas. Dalam serangan phishing email, penyerang mengirimkan email yang tampaknya berasal dari organisasi terkemuka seperti bank, bisnis, lembaga pemerintah, atau penyedia layanan internet dalam email tersebut anda akan diarahkan untuk membuka link dari tautan yang dikirimkan.

Tujuan utama phishing email adalah mencuri informasi pribadi, seperti sandi, nomor kartu kredit, atau informasi akun keuangan, atau membuat pengguna mengklik tautan berbahaya atau membuka lampiran berbahaya. Penyerang sering menggunakan teknik psikologis dan manipulatif untuk mempengaruhi korban sehingga tetap dalam perjalanan serangan mereka.

Berikut adalah beberapa karakteristik umum dari skema phishing email:

a. Pengiriman Email Palsu: Pengirim membuat email dengan baris dan format subjek tertentu yang diakui oleh organisasi terpercaya atau terkenal. Mereka bisa menggunakan logo, alamat email pribadi, atau bahasa yang cocok untuk komunikasi langsung yang realistis.
b. Phishing email sering menggunakan baris subjek yang mengancam, seperti "Peringatan Penting" atau "Tindakan Darurat," untuk mengelabui penerima agar berpikir bahwa mereka harus merespons atau mengunduh tindakan yang ditargetkan.
c. Permintaan Informasi Pribadi: Pelaku dapat meminta penerima email untuk memasukkan informasi sensitif seperti nama, nama belakang, nomor kartu kredit, atau informasi akun lainnya. Mereka sering menggunakan alasan palsu, seperti keamanan pembaruan atau verifikasi akun, untuk mendapatkan informasi yang diminta.
d. Tautan berbahaya: Phishing email sering berisi tautan yang mengarahkan pengguna ke situs web berbahaya yang dirancang untuk mengelabui mereka agar memasukkan informasi pribadi mereka. Kutipan ini mungkin tersembunyi dalam teks atau gambar dan secara konsisten dan tidak masuk akal.
e. Lampiran berbahaya: Email phishing juga dapat berisi lampiran berbasis malware, seperti virus. Jika pengguna mengaktifkan dan menggunakan malware yang dimaksud, perangkat dapat terinfeksi dan data sensitif mungkin perlu diamankan, atau perangkat mungkin tidak berfungsi.

Ada beberapa metode yang dapat anda gunakan untuk melindungi diri dari phishing email:

a. Verifikasi pengirim: Periksa alamat email pengirim dengan cermat dan asumsikan bahwa itu berasal dari sumber yang dapat dipercaya. Jika ada perbedaan, konfirmasikan menggunakan saluran komunikasi yang andal, seperti menghubungi perusahaan secara langsung atau mengunjungi situs web resmi mereka.
b. Jangan klik pesan peringatan: Jika email berisi peringatan, jangan klik dengan cepat. Demikian pula, gerakkan kursor ke tautan yang relevan tanpa mengkliknya untuk melihat URL yang jelas. Harus diasumsikan bahwa itu tidak tepat dan dapat mengganggu situasi.
c. Berhati-hatilah saat menangani informasi sensitif: Hindari mengirim informasi pribadi atau keuangan melalui email. Pebisnis yang cerdas tidak akan meminta informasi pribadi melalui email.
d. Ingat bahasa dan tujuan email: Periksa tujuan email, tata bahasa yang buruk, atau penggunaan bahasa yang aneh. Phishing email sering mengandung seluk-beluk atau petunjuk lain yang dapat dideteksi jika dikenali dengan pasti.
e. Gunakan perangkat lunak keamanan saat ini: Pastikan jaringan anda dilindungi oleh perangkat lunak keamanan saat ini yang kuat, seperti pemindai phishing email.
f. Jelaskan kesadaran: Agar lebih waspada dan sadar saat berinteraksi dengan email phishing, mendidik diri sendiri

dan orang lain tentang taktik dan karakteristik phishing email.

3. **Smishing Phishing**

Source: https://us.norton.com/content/dam/blogs/images/norton/am/smishing-attacks-explained.png

Smishing Phishing adalah teknik yang digunakan untuk menggambarkan serangan phishing yang menggunakan pesan teks (SMS) sebagai sarana untuk mengidentifikasi target. Pelaku smishing memancing korban agar memberikan informasi pribadi atau mengunjungi situs web palsu, atau mengirimkan pesan

teks palsu yang terlihat seperti pesan resmi dari lembaga atau perusahaan terpercaya.

Berikut adalah contoh pekerjaan sehari-hari yang dilakukan oleh smishing phishing:

a. Pesan Teks Palsu: Pelaku akan mengirimkan pesan teks palsu yang menyampaikan rasa urgensi atau kebutuhan untuk tindakan segera sehingga korban dapat mulai menghapus tindakan. Ada kemungkinan bahwa pesan tersebut berisi informasi palsu tentang pemblokiran akun, transaksi yang dipertanyakan, atau keputusan yang dipertanyakan. Pesan juga dapat menegaskan bahwa korban harus menyembunyikan informasi pribadi atau bahwa perlu untuk mendatangkan hal yang dibutuhkan.
b. Tautan atau Nomor Telepon Palsu: Pesan smishing secara teratur berisi tautan yang tertaut ke situs web atau nomor telepon palsu. Pelaku smishing memiliki keyakinan bahwa korban akan mengklik peringatan atau memanggil nomor tersebut. Sementara nomor telepon dapat menghubungkan pesanan ke operator jarak jauh yang bersedia menangani informasi sensitif, tautan dapat mengirim pesanan ke situs web yang dirancang khusus untuk mencuri informasi pribadi.
c. Permintaan Informasi: Pelaku dapat meminta subjek untuk memberikan informasi pribadi seperti kata sandi, nomor kartu kredit, informasi rekening bank, atau informasi pengenal lainnya. Pelaku berharap bahwa korban akan memberikan informasi ini sambil sepenuhnya memahami bahwa sumber pesan adalah sumber terpercaya.

d. Ancaman atau Imbauan: Pesan smishing juga dapat berisi ancaman atau imbauan palsu untuk memaksa korban mengambil tindakan. Misalnya, pesan tersebut dapat mengancam akan memblokir akun atau menghentikan layanan jika korban tidak memberikan informasi yang diminta.

Berikut adalah beberapa opsi yang perlu dipertimbangkan untuk melindungi diri anda dari smishing phishing :

a. Waspadai Pesan Teks yang Mencurigakan: Jangan menunggu untuk mengirimkan tindakan Anda jika Anda menerima pesan teks yang mencurigakan. Waspadai pesan yang meminta informasi privas atau menawarkan satu yang terlalu baik untuk mendapat kenyataan. Jangan klik tautan atau nyalakan lampu dari teks yang tidak dapat dipahami.
b. Memverifikasi Identitas Pengirim: Jika Anda mendapatkan materi tertulis dari organisasi atau organisasi label resmi, konfirmasikan identitas pengirim sebelum memberikan informasi pribadi apa pun. Hubungi perusahaan atau organisasi secara langsung menggunakan nomor telepon yang ditampilkan di situs web resmi mereka untuk memverifikasi jumlah terutang.
c. Keamanan Informasi: Jangan pernah membocorkan informasi pribadi melalui pesan teks, seperti nomor kartu kredit anda, sandi, atau detail keuangan lainnya. Perusahaan yang dapat dipercaya tidak akan meminta informasi pribadi melalui teks.
d. Periksa Situs Web dengan Sertifikat: Jika sepotong teks mengarahkan anda ke situs web tertentu, periksa dengan

URL sertifikat dan anggap itu adalah situs web resmi. Hindari memasukkan informasi pribadi di situs web yang tidak aman atau tidak memiliki keamanan yang tepat.

e. Manfaatkan Aplikasi Keamanan: Instal aplikasi keamanan di smartphone anda yang terkunci serta dapat mendeteksi dan memblokir teks berbahaya. Beberapa aplikasi keamanan juga dapat memberikan informasi tentang teks pesan yang mencurigakan.

f. Melaporkan Serangan: Jika anda menerima email phishing, beri tahu penyedia layanan telepon anda serta cabang lokal dari penyedia hukum. Melaporkan serangan dapat membantu mencegah seseorang menargetkan orang lain.

g. Pendidikan: Terus tingkatkan pemahaman anda tentang phishing, smishing, dan taktik penipu lainnya. Mengikuti peristiwa terkini dan informasi keamanan akan membantu anda tetap mengikuti peristiwa yang terjadi dalam teknologi digital.

Dengan mengikuti petunjuk yang diberikan, anda dapat mengurangi risiko menjadi korban penipuan smishing phishing. Selalu berhati-hati dan waspada saat membaca bagian teks yang mengandung tautan berbahaya dan pastikan untuk melindungi informasi pribadi anda.

4. Vishing Phishing

Source: https://pimages.toolbox.com/wp-content/uploads/2022/05/09122828/Vishing-Attack-Mechanism.png

Vishing *(Voice Phishing)* adalah jenis serangan phishing yang menggunakan telepon panggilan untuk mengelabui korban agar memberikan informasi pribadi atau uang. Pelaku phishing sering menyamar sebagai perwakilan dari lembaga keuangan, bank, atau bisnis lain yang sah untuk mendapatkan kepercayaan klien.

Berikut adalah beberapa informasi tentang Vishing Phising :

a. Modus Operandi: Vishing phisher menggunakan telepon panggilan untuk terhubung dengan target. Mereka akan bertindak jujur dan tidak memihak sebagai karyawan

bisnis terkemuka seperti bank, penyedia kartu kredit, atau lembaga mata uang lainnya. Dalam panggilan yang disebutkan di atas, mereka akan menunjukkan perasaan urgensi dan mempertimbangkan untuk mengintimidasi orang banyak untuk mendapatkan informasi sensitif seperti nomor rekening, kata sandi, atau kode keamanan.

b. Memanipulasi Emosi: Pelaku phishing sering menggunakan teknik manipulasi emosional untuk menyakiti target. Mereka memiliki kemampuan untuk menyembunyikan penutupan akun yang akan datang, menyangkal adanya transaksi yang dipertanyakan, atau memberikan peringatan tentang peluang investasi yang akan datang. Tujuan mereka adalah membuat orang gugup atau cemas sehingga korban dapat membocorkan informasi rahasia.

c. Phishing Identitas: Pelaku phishing sering menggunakan teknik spoofing untuk menyembunyikan identitas asli mereka dan membuat nomor telepon mereka tampak berasal dari organisasi atau bisnis yang sepenuhnya berafiliasi dengan mereka. Ini memberi pengguna dorongan kepercayaan diri dan membuat mereka lebih mungkin memberikan informasi sensitif.

d. Permintaan Informasi: Dalam sejumlah skenario phishing, pengguna dapat meminta panggilan untuk mendapatkan informasi yang dicari phisher. Informasi yang bersifat rahasia dapat digunakan untuk verifikasi identitas atau tujuan penipuan di masa mendatang.

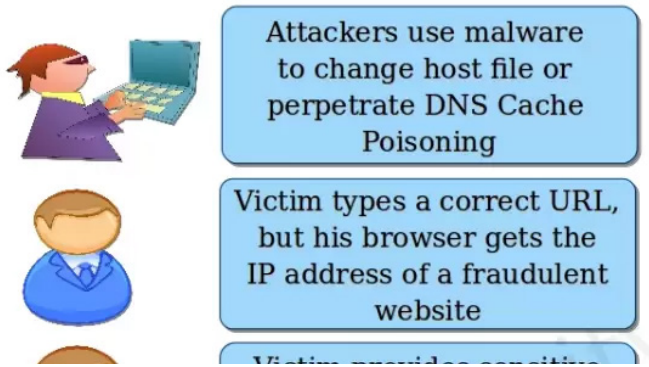
Berikut adalah beberapa opsi yang perlu dipertimbangkan untuk melindungi diri anda dari serangan Vhising Phising :

a. Verifikasi Identitas: Jika Anda menerima panggilan yang mengancam, tanyakan identitas lengkap orang yang mengirimnya dan verifikasi. Jangan takut untuk meminta timeline yang lebih panjang dan konfirmasi konfirmasi panggilan kebenaran.
b. Jangan Berikan Informasi Pribadi: Jangan berikan informasi sensitif melalui panggilan telepon yang tidak dapat dibedakan dari tujuan penggunaannya, seperti nomor kartu kredit Anda, nama Anda dalam huruf kapital, atau kode PIN Anda.
c. Hubungi Pihak yang Diklaim: Jangan memberikan informasi langsung ke penelepon jika panggilan terkait dengan akun atau layanan tertentu. Alias, dapatkan nomor telepon asli dari perusahaan atau organisasi yang relevan dari sumber yang memiliki reputasi baik, lalu hubungi mereka untuk mengonfirmasi kemajuan aplikasi.
d. Pengumpulan Informasi: Penting untuk terus mengumpulkan informasi pribadi Anda. Jangan membagikan informasi sensitif kepada pihak yang tidak dapat dipercaya atau melalui saluran komunikasi yang tidak aman.
e. Melaporkan Serangan: Jika anda menerima email phishing, beri tahu penyedia layanan telepon anda serta cabang lokal dari penyedia hukum. Melaporkan serangan dapat membantu mencegah seseorang menargetkan orang lain.

Dengan mengikuti petunjuk yang diberikan, anda dapat mengurangi risiko menjadi korban penipuan vishing phishing. Selalu berhati-hati dan waspada saat membaca bagian teks yang

mengandung tautan berbahaya dan pastikan untuk melindungi informasi pribadi anda.

5. Pharming Phishing



Source: https://www.thesecuritybuddy.com/wordpress/bdr/uploads/2020/01/Pharming_20.jpg.webp

Pharming Phising dilakukan ketika pelaku memilih untuk mengirim korban ke situs web palsu tanpa terlebih dahulu mengizinkan tautan yang dikirim melalui pesan diterima. Untuk mengakses situs web, pelaku menggunakan teknik seperti keracunan cache DNS (Domain Name System) atau serangan man-in-the-middle.

Pharming phishing juga dikenal sebagai phishing DNS, adalah jenis serangan phishing yang bertujuan untuk memikat pengguna ke situs web yang disusupi tanpa membiarkan mereka melihat jejak apa pun yang dikirimkan menggunakan pesan asli dan tanpa sepengetahuan mereka. Dalam serangan phishing, penyerang menggunakan DNS (Domain Name System) atau

cache DNS pada perangkat jaringan atau server untuk mengelabui pengguna agar mengunjungi situs web berbahaya.

DNS adalah sistem yang memetakan nama domain (seperti www.example.com) ke alamat IP yang sesuai. Ketika pengguna memasukkan URL untuk situs web tertentu, DNS digunakan untuk mencari alamat IP yang terkait dengan domain yang dimaksud sehingga pelaku dapat terhubung ke situs web yang diinginkan.

Penyerang dapat melakukan salah satu dari dua bentuk serangan dalam serangan pharming phishing:

a. DNS Cache Poisoning: Penyerang mengeksploitasi kelemahan dalam sistem DNS, yang menyebabkan penyimpanan DNS cache yang dikendalikan oleh ISP atau server jaringan agar dapat diisi dengan informasi palsu. Ketika pengguna memasukkan URL untuk situs web yang aman, sistem DNS menarik alamat IP pengguna dari cache yang baru saja dibersihkan, mengarahkan korban ke situs web yang aman.
b. Malware: Pelaku menginfeksi perangkat nirkabel pengguna dengan malware yang mengganggu pengaturan DNS perangkat. Ketika pengguna memasukkan URL untuk situs web yang aman, perangkat yang terinfeksi akan memperingatkan mereka dan kemudian mengarahkan mereka ke situs web aman yang telah diidentifikasi oleh penyerang.

Tujuan utama serangan phishing adalah untuk mencuri informasi pengguna yang sensitif seperti nama, kata sandi, atau informasi keuangan korban. Situs web yang dibuat oleh pemula

sering menggunakan situs web aman, seperti situs perbankan atau e-commerce, untuk mengelabui pengguna agar mengungkapkan informasi pribadi mereka.

Langkah berikut dapat digunakan oleh pengguna untuk melindungi diri dari serangan pharming phishing :

a. Memanfaatkan perangkat lunak keamanan dengan sistem terkini dan memperbarui sistem operasi secara tepat waktu.
b. Verifikasi URL situs web dengan hati-hati dan pertimbangkan apakah ada perbedaan atau potensi risiko keamanan.
c. Gunakan DNS yang dapat dipercaya dan periksa pengaturan DNS pada setiap router untuk memastikan tidak ada perubahan yang salah telah dilakukan.
d. Manfaatkan VPN *(Virtual Private Network)* untuk mengamankan koneksi internet dan mencegah serangan phishing.
e. Menghindari mengklik tautan yang mencurigakan, yang dikirim melalui email, atau yang tak diketahui, atau pesan yang tak diketahui.
f. Laporkan aktivitas phishing yang mencurigakan ke penyedia layanan internet atau administrator jaringan.

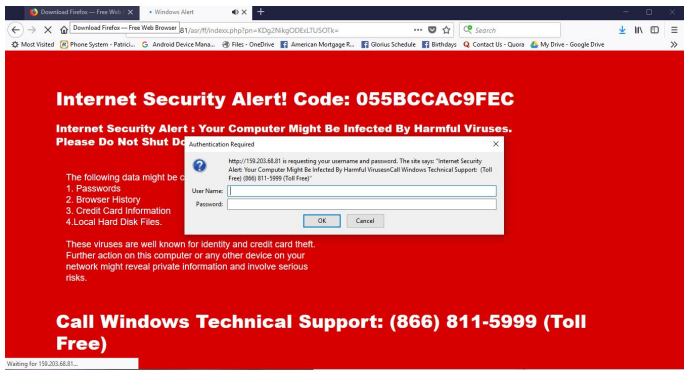
6. HTTPS Phishing

Source: https://dewailmu.id/wp-content/uploads/2019/04/facebook-phising.png.webp

Phishing HTTPS, juga dikenal sebagai phishing HTTPS, adalah jenis serangan phishing yang mendorong pengguna untuk menggunakan protokol HTTPS untuk melindungi informasi sensitif dari pengguna, seperti kata sandi, informasi keuangan, atau data pribadi. HTTPS adalah protokol aman yang digunakan untuk membatasi komunikasi antara pengguna dan situs web dengan memanfaatkan enkripsi data. Serangan HTTPS phishing dilakukan dengan mengirimkan email kepada korban yang berisi tautan ke situs web berbahaya. Situs web ini juga dapat digunakan untuk menjerat korban dan mengungkapkan informasi pribadi mereka.

Pada kenyataannya, dalam serangan phishing HTTPS, penyerang membuat situs web berbahaya yang meniru situs web yang sah dan dapat dipercaya, seperti lembaga keuangan atau platform jejaring sosial. Pelaku membuat koneksi aman (HTTPS) dengan pengguna dengan menggunakan sertifikat SSL/TLS yang valid atau palsu, menciptakan rasa percaya dan meyakinkan pengguna bahwa situs web tersebut adalah asli dan dapat dipercaya.

7. Pop-Up Phishing



Source: https://assets-prod.sumo.prod.webservices.mozgcp.net/media/uploads/images/thumbnails/2017-12-01-09-41-11-e45030.png

Pop-up phishing adalah jenis phishing di mana penyerang menggunakan jendela pop-up untuk mendapatkan informasi sensitif dari korban. Ketika pengguna mengakses situs web yang telah disusupi atau telah tercemar oleh malware, jendela pop-up dengan tujuan mengumpulkan data sensitif, seperti nama pengguna, skrip sandi, atau informasi keuangan, muncul.

Biasanya, phishing pop-up terjadi ketika pengguna mengklik tautan berbahaya atau memasuki situs web yang telah disusupi.

Ketika pengguna berinteraksi dengan situs web atau artikel yang disebutkan di atas, jendela pop-up muncul dan dapat menampilkan input pengguna yang tidak menyenangkan atau permintaan informasi pribadi.

Phishing pop-up dapat menonaktifkan halaman online yang aman atau menggunakan logo dan grafik lainnya untuk membuatnya tampak mencurigakan. Juga sering digunakan oleh mereka adalah metode psikologis 'mancing pengguna' untuk memberikan informasi yang akurat. Misalnya, phishing pop-up mungkin mengklaim bahwa pengguna telah menerima uang, menerima pemberitahuan khusus, atau menggunakan penipuan untuk memblokir akses ke akun mereka sampai mereka memberikan informasi palsu.

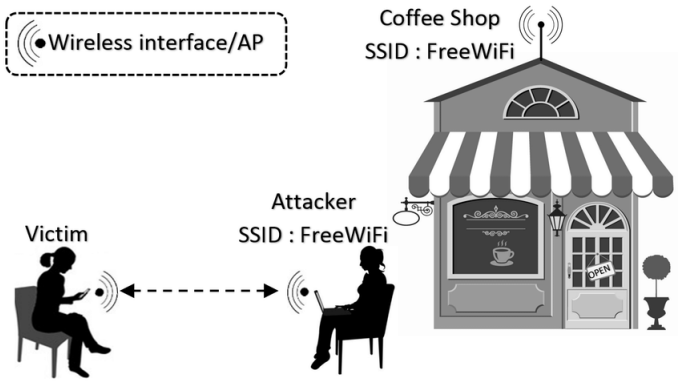
Ada beberapa metode yang dapat Anda gunakan untuk melindungi diri dari phishing pop-up :

a. Saat memasuki situs web atau berinteraksi dengan pesan, berhati-hatilah terhadap iklan pop-up yang sesekali muncul.
b. Jangan memberikan informasi pribadi atau informasi keuangan melalui jendela pop-up yang mengganggu.
c. Gunakan alat pencegahan phishing yang tepercaya dan terkini untuk melindungi diri Anda dari serangan phishing pop-up.
d. Jangan klik tautan yang menyinggung atau tidak dapat dikenali, terutama jika muncul di jendela pop-up.
e. Jika Anda menemukan jendela pop-up yang menyebabkan masalah, tutup dengan mengklik tombol "X" yang terlihat

di sudut kanan atas jendela, lalu klik dengan hati-hati tombol atau simbol lain di dalam jendela itu sendiri.

f. Penting untuk selalu berhati-hati dan waspada terhadap aktivitas situs web yang mencurigakan serta pesan yang muncul di jendela pop-up. Jika Anda mencurigai phishing pop-up, pastikan untuk melaporkan kejadian tersebut kepada otoritas yang sesuai atau penyedia layanan.

8. Evil Twin Phishing



Source: https://www.researchgate.net/profile/Omar-Nakhila/publication/321122614/figure/fig5/AS:631949064421377@1527679806852/Illustration-of-an-Evil-Twin-Attack-The-attacker-can-successfully-lure-a-victim-into.png

Evil twin phishing adalah jenis phishing di mana penyerang menciptakan jaringan Wi-Fi yang tampaknya sah dan diketahui oleh pengguna. Penyerang membantu mereka untuk terhubung ke jaringan palsu dengan menipu mereka dengan nama jaringan yang sama atau mirip dengan jaringan Wi-Fi yang ada di sekitar pengguna.

Proses phishing kembar jahat dimulai dengan penyerang membuat hotspot Wi-Fi dengan nama yang menarik (SSID), sering menggunakan nama umum untuk jaringan, seperti nama kafe, hotel, atau tempat umum lainnya. Saat mencari jaringan Wi-Fi yang tersedia, jaringan palsu yang dibangun penyerang akan muncul di hasil. Karena nama jaringan palsu cocok atau mirip dengan nama jaringan Wi-Fi yang diharapkan mesin pencari untuk digunakan pengguna, pengguna akan enggan untuk terhubung ke jaringan palsu.

Tujuan utama dari Evil Twin Phishing adalah untuk mendapatkan informasi pengguna yang dapat digunakan untuk tujuan ilegal, seperti pencurian identitas atau penipuan keuangan, seperti nama pengguna, alamat email, atau kata sandi.

Untuk melindungi diri anda dari Evil Twin Phishing, berikut ini adalah beberapa opsi untuk dipertimbangkan:

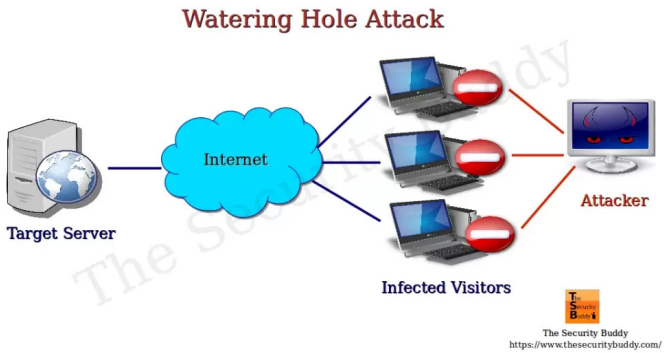
a. Gunakan jaringan WiFi yang dapat dipercaya dan aman, seperti yang ada di rumah, kantor, dan hotspot publik yang telah menjalani verifikasi.
b. Sebelum menghubungkan, periksa jaringan Wi-Fi yang tersedia dengan mencari nama cermat. Pastikan jaringan yang anda gunakan aman dan disiapkan oleh pihak yang dapat dipercaya.
c. Tanyakan hewan peliharaan atau anggota staf yang antusias tentang lokasi jika anda memiliki pertanyaan tentang stabilitas jaringan Wi-Fi.
d. Jangan pernah memberikan informasi sensitif atau masuk ke situs web yang berisi data sensitif saat terhubung ke jaringan Wi-Fi publik.

a. Gunakan Jaringan Pribadi Virtual (VPN) yang aman saat terhubung ke jaringan Wi-Fi publik. VPN membantu anda melindungi koneksi internet anda dengan mengenkripsi komunikasi anda dan mengamankan data sensitif dari potensi ancaman terdekat.

b. Perbarui perangkat lunak dan aplikasi keamanan anda secara teratur untuk melindungi dari penyerang Evil Twin kerentanan yang diketahui dengan dapat dimanfaatkan.

c. Anda dapat mengurangi risiko menjadi korban serangan Evil Twin Phishing dengan mengikuti protokol aman saat terhubung ke jaringan WiFi.

9. Watering Hole Phishing



Source: https://www.thesecuritybuddy.com/wordpress/bdr/uploads/2020/02/WateringHoleAttack_20.jpg.webp

Watering hole phishing adalah jenis serangan phishing di mana penyerang menargetkan kelompok pengguna tertentu dengan menyamarkan dan menyerang situs web yang sering menerima kunjungan dari grup tersebut. Penyerang mengidentifikasi situs web yang dikunjungi oleh anggota target,

seperti situs web perusahaan, forum industry, atau situs web komunitas, dan kemudian menginfeksi situs tersebut dengan malware atau menggantikan kontennya dengan konten yang dirancang untuk mencuri informasi.

Watering hole phishing dimulai dengan pelaku melakukan penelitian dan analisis pada kelompok sasaran untuk mengidentifikasi situs web yang sering mereka kunjungi. Penyerang kemudian mempertimbangkan untuk mengidentifikasi kerentanan di lokasi yang disebutkan di atas atau bekerja sama dengan organisasi yang memiliki akses ke sana untuk menginfeksi situs web dengan malware.

Ketika anggota kelompok sasaran memasuki lokasi yang terinfeksi, mereka tampaknya tidak berada dalam bahaya. Situs web yang terinfeksi dapat melakukan berbagai tindakan berbahaya, termasuk memasang ekstensi berbahaya di komputer pengguna, melindungi informasi sensitif atau uang, atau mengizinkan akses tidak sah ke sistem atau akun mereka.

Watering hole phishing cukup efektif karena menargetkan kelompok sasaran pengguna dan memanfaatkan kepercayaan yang ditunjukkan pengguna untuk situs web yang sering mereka kunjungi. Saat mengakses situs web yang aman dan terpercaya, pengguna cenderung sedikit lebih waspada, membuat mereka lebih rentan terhadap jenis phishing ini.

Berikut ini adalah beberapa opsi untuk melindungi diri anda dari phishing lubang air :

a. Perbarui dan gunakan sistem keamanan perangkat lunak yang andal untuk mendeteksi dan menghilangkan malware.

b. Pastikan senjata dan benda tajam Anda selalu memiliki patch terbaru yang tersedia.
c. Hindari mengunjungi situs web yang curang atau tidak dapat dipercaya.
d. Selalu waspada terhadap perubahan atau penyimpangan pada website yang sering Anda kunjungi.
e. Gunakan langkah-langkah keamanan jaringan yang kuat, seperti firewall dan sistem deteksi intrusi (IDS / IPS), untuk memfilter dan memblokir akses ke situs web yang aman.
f. Memanfaatkan teknologi sandboxing atau server virtual untuk meluncurkan situs web yang berbahaya atau tidak dapat diandalkan di lingkungan yang tidak bersahabat.
g. Mendidik diri sendiri dan anggota lain dari kelompok Anda tentang bahaya email phishing dan prosedur keamanan digital yang efektif.
h. Anda dapat membantu diri Anda merasa lebih aman dengan mengadopsi prosedur keselamatan yang baik dan meningkatkan kesadaran tentang insiden phishing.

10. Whaling Phishing

Source: https://www.pandasecurity.com/en/mediacenter/src/uploads/2022/12/detecting-whaling.png

Whaling Phishing adalah jenis serangan siber yang menargetkan individu atau karyawan bernilai tinggi di dalam suatu organisasi. Ini adalah jenis phishing yang lebih canggih dan ditargetkan di mana penyerang menargetkan korban dan menggunakan taktik untuk mengambil keuntungan dari posisi kelemahan korban.

Saat terlibat dalam whaling phishing, penyerang biasanya menyamar sebagai orang resmi atau dapat dipercaya, seperti CEO, CFO, atau eksekutif lain, untuk mengelabui target agar mengirimi mereka uang. Mereka menggunakan berbagai teknik rekayasa sosial, seperti spoofing email, untuk membuat pidato mereka terdengar meyakinkan. Email yang dimaksud sering berisi permintaan yang sensitif atau mengancam, dengan tujuan memanipulasi penerima untuk mengungkapkan informasi rahasia atau melakukan tindakan tertentu yang dapat membahayakan pengirim.

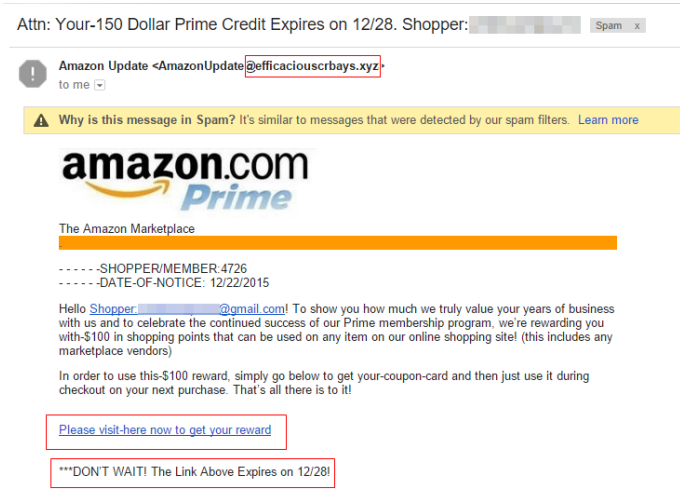
Tujuan utama whale phishing adalah untuk mendapatkan akses ke informasi keuangan, informasi akun, atau informasi login yang aman tanpa terdeteksi. Penyerang dapat memilih untuk mengelabui seseorang agar memberi mereka informasi login, informasi keuangan, atau detail penting lainnya dengan mengarahkan mereka ke situs web palsu yang sangat mirip dengan yang asli. Mereka juga dapat menggunakan malware atau email phishing untuk membahayakan jaringan atau sistem yang digunakan oleh militer.

Serangan whiling phishing sering membutuhkan penelitian dan pengakuan yang signifikan dari administrasi perburuan paus. Mereka memberikan rincian tentang peran, tanggung jawab, koneksi, dan kegiatan korban yang sedang berlangsung untuk membuat pesan mereka sendiri lebih meyakinkan. Ini dapat mengurangi informasi yang tersedia untuk umum dari profil media sosial, situs web perusahaan, atau kebocoran data historis.

Individu dan organisasi harus waspada dan mematuhi praktik keamanan email terbaik untuk melindungi diri dari phishing perburuan paus:

a. Pendidikan dan Pembelajaran: Pelajari tentang risiko yang terkait dengan perburuan paus, cara mengidentifikasi email yang mencurigakan, dan pentingnya memverifikasi secara menyeluruh setiap permintaan informasi sensitif.
b. Autentikasi Kuat: Gunakan otentikasi multi-faktor (MFA) untuk mengakses sistem dan akun penting untuk meningkatkan integritas dokumen.
c. Gunakan filter email jabat tangan dan sistem antivirus lunak untuk mendeteksi dan memblokir email phishing dan lampiran berbahaya lainnya.
d. Prosedur Verifikasi: Gunakan prosedur verifikasi yang jelas untuk permintaan yang mencakup informasi sensitif, terutama untuk transaksi keuangan. Gunakan sistem pemeriksaan dan keseimbangan untuk mengkonfirmasi validitas permintaan.
e. Pembaruan dan Patching Berkala: Selalu tambal setiap komponen lunak, termasuk sistem operasi, server web, dan komponen lunak keamanan, untuk melindungi diri Anda dari kerentanan yang telah diidentifikasi.
f. Rencana Tanggap Kejadian: Siapkan rencana untuk mengatasi dan mengurangi ancaman perburuan paus dengan cepat. Ini termasuk mendokumentasikan setiap penyimpangan, menyelesaikan sistem yang salah, dan melakukan penyelidikan forensik.
g. Individu dan organisasi dapat mengurangi risiko menjadi korban phishing dengan menggunakan bahasa ini dan berfokus pada praktik komunikasi email hat-trick.

11. Clone Phishing



Source: https://www.kratikal.com/blog/wp-content/uploads/2019/11/Phishing-example-Amazon-Prime-22-12-2015.png

Clone phishing adalah jenis phishing yang melibatkan perolehan informasi sensitif melalui email, situs web, atau dokumen asli. Penyerang menciptakan salinan yang sangat mirip dengan yang asli untuk menipu korban dalam serangan ini.

Prosedur kloning phishing dimulai dengan pengguna memasukkan alamat email mereka atau membuka dokumen resmi yang mencurigakan. Kemudian mereka membuat salinan yang hampir identik dalam konten dan tata letak. Zat ini sering digunakan sedikit untuk memunculkan unsur penipuan, seperti tautan atau lampiran.

Setelah salinan palsu selesai dibuat, penyerang mengirimkannya ke pelanggan melalui email atau bentuk komunikasi langsung lainnya. Email atau surat yang disebutkan

di atas sering mencoba meyakinkan penerima bahwa itu berasal dari sumber yang dapat dipercaya, seperti bank, layanan internet, atau perusahaan terkenal. Pesan yang disebutkan di atas dapat berisi permintaan untuk memverifikasi informasi pribadi, mengubah ejaan kata, atau melakukan beberapa tindakan spesifik lainnya yang akan menguntungkan penyerang.

Seorang korban yang tidak langsung merespon nantinya bisa mengklik link di email yang bersangkutan atau menggunakan lampiran yang disediakan. Tautan yang disebutkan di atas akan mengarahkan pengguna ke situs web palsu yang sebanding dengan situs web internasional di mana mereka akan diminta untuk memasukkan informasi sensitif seperti nama, kata sandi, atau nomor akun mereka. Jika korban menembakkan lampu yang berada di sisi atas, itu dapat menginfeksi komputer korban dengan malware atau router yang terinfeksi.

Adapun pencegahan yang dapat dilakukan untuk Clone Phishing :

a. Waspadai Email yang Mencurigakan: Waspadalah terhadap email yang berisi informasi sensitif atau yang cermat dan mencurigakan. Waspadai perbedaan alamat email pengirim, salah pengejaan, atau tatabahasa kesalahan, dll.
b. Aturan Verifikasi: Jangan ragu untuk terlibat dalam percakapan atau memberikan informasi rahasia jika Anda menerima email yang menyinggung. Verifikasi validasi email Anda dengan menekan nomor terpercaya secara diam-diam menggunakan saluran komunikasi sebelumnya yang Anda gunakan.

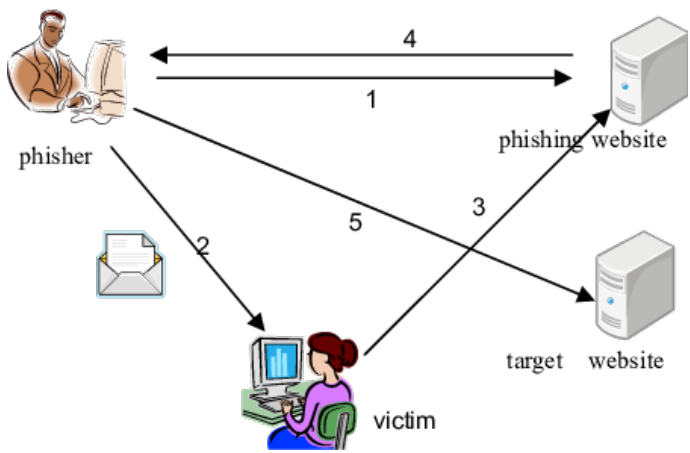
c. Harap Perhatikan URL: Sebelum memasukkan informasi sensitif atau mengklik tautan, periksa alamat URL dengan kapitalisasi yang sama. Jangan melanjutkan jika ada perbedaan atau tanda-tanda yang mengkhawatirkan.

d. Selalu perbarui perangkat lunak, termasuk sistem operasi dan keamanan perangkat lunak, untuk melindungi diri dari kerentanan tersebut di atas.

e. Pelajari lebih lanjut tentang penipuan phishing: Untuk lebih memahami teknik dan taktik phishing serta untuk dapat mengenali potensi ancaman, tingkatkan kesadaran Anda terhadapnya.

Dengan berhati-hati dalam teknik clone phishing, Anda dapat melindungi diri dari serangan itu dan mengurangi risiko informasi pribadi Anda.

12. Deceptive Phishing



Source: https://www.researchgate.net/profile/Huajun-Huang-4/publication/224602500/figure/fig1/AS:340327241142284@1458151745680/steps-in-a-deceptive-phishing-attack.png

Deceptive Phishing adalah jenis phishing yang menggunakan tipu daya dan manipulasi untuk mengelabui pengguna agar memberikan informasi pribadi. Dalam situasi ini, tujuannya adalah untuk membuat target memahami bahwa mereka berurusan dengan entitas yang dapat dipercaya seperti bank, layanan internet, atau perusahaan terkenal.

Penyerang membuat pesan atau situs online palsu terlihat meyakinkan dengan berbagai teknik. Mereka sering menggunakan elemen desain, logo yang mirip, dan bahasa dengan aslinya. Pesan atau website palsu dalam hal ini seringkali memiliki anggaran tingkat rupa, sehingga jelas dan tidak ambigu bagi pelanggan.

Phishing yang menipu sering menggunakan teknik manipulasi emosional. Penyerang dapat mengambil manfaat dari kekhawatiran, mendesak, atau ancaman untuk melemahkan korban. Mereka mampu membayangkan skenario yang mungkin menyulitkan seseorang untuk melakukan tindakan yang diinginkan, seperti mengirimkan informasi pribadi atau melakukan pembayaran.

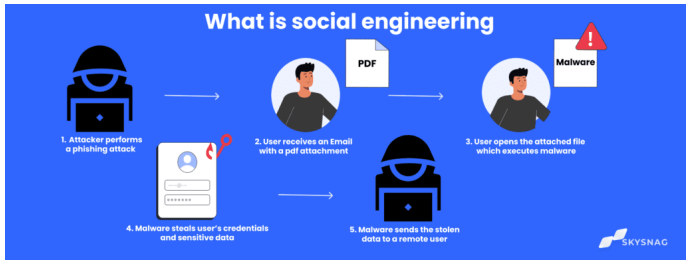
Contoh phishing yang menyesatkan dapat memberikan penawaran eksklusif atau penawaran menarik yang meminta penerima untuk mengisi formulir dengan informasi pribadi mereka. Atau, masalahnya mungkin pesan yang memperingatkan bahwa lembaga uang akan menutup rekening korban sampai mereka memverifikasi saldo rekening mereka menggunakan tautan yang tersedia.

Berikut adalah beberapa opsi yang perlu dipertimbangkan untuk melindungi diri Anda dari phishing yang menyesatkan:

a. Waspada Pesan: Perhatikan pesan yang mengandung ancaman, tekanan mendesak, atau tawaran yang sangat cocok untuk dijadikan pernyataan. Jangan memberikan informasi pribadi atau melakukan kegiatan terlarang.
b. Verifikasi Sumber: Jika Anda mendapatkan pesan yang menjengkelkan, konfirmasikan validitas pesan dengan berbicara dengan pelanggan tepercaya secara pribadi menggunakan saluran komunikasi sebelumnya. Harap jangan menggunakan nomor telepon atau kode yang disediakan di pesan yang disebutkan di atas.
c. Perhatikan alamat email dan URL: Periksa alamat email pengirim dan URL situs web dengan hati-hati. Sedikit perbedaan dalam pengejaan atau tanda-tanda yang menimbulkan kekhawatiran dapat mengindikasikan bahwa itu adalah pesan atau situs palsu.
d. Berhati-hatilah dengan Tautan dan Lampiran: Jangan klik tautan atau aktifkan lampiran dari pesan kursor. Ejekan yang disebutkan di atas dapat mengarahkan Anda ke situs web berbahaya atau memperkenalkan malware ke sistem Anda.
e. Pelajari tentang teknik dan strategi yang digunakan dalam phishing, termasuk phishing yang menyesatkan, untuk memahami dan mengenali potensi penipuan.

Dengan meningkatkan kewaspadaan Anda, memantau aktivitas online Anda, dan menolak memberikan informasi pribadi kepada siapa pun yang tidak dapat dipercaya, Anda dapat melindungi diri dari serangan phishing yang curang dan meningkatkan keamanan online Anda.

13. Social Engineering Phishing



Source: https://www.skysnag.com/wp-content/uploads/2022/10/Frame-523What-is-social-engineering-3-1536x578.png

Phishing rekayasa sosial adalah jenis phishing yang melibatkan manipulasi psikologis korban untuk mendapatkan informasi sensitif atau memanipulasi mereka untuk melakukan tindakan yang ditargetkan. Dalam hal ini, penyerang menggunakan teknik re-etika sosial untuk menghilangkan korban.

Skema phishing termasuk rekayasa sosial sering dimulai dengan pengumpulan informasi target, baik melalui saluran terbuka seperti media sosial atau dengan teknik alternatif seperti pengumpulan data atau infiltrasi. Penyerang menggunakan informasi ini untuk memanfaatkan kepercayaan korban atau pesan atau skenario yang terlihat meyakinkan.

Penyerang dapat mengidentifikasi sebagai orang terkenal atau pengamat yang telah menarik perhatian, seperti supervisor pekerjaan, anggota tim TI, atau perwakilan dari layanan klien. Untuk berkomunikasi dengan korban, mereka menggunakan email, teks tertulis, panggilan telepon, atau bentuk alternatif dari saluran komunikasi.

Tujuan penipuan phishing manipulasi psikologis mungkin berbeda. Beberapa contoh tujuan kalimat ini adalah sebagai berikut:

a. Memperoleh Informasi Pribadi: Dengan mengidentifikasi diri mereka sebagai pelanggan bank atau layanan online, seseorang dapat memilih untuk mencari informasi pribadi seperti nomor kartu kredit, nomor jaminan sosial, atau informasi di rekening bank mereka.
b. Seseorang dapat menggunakan teknik rekayasa sosial untuk meyakinkan korban untuk memberi mereka akses ke jaringan atau sistem perusahaan, yang dapat digunakan untuk melindungi data atau melakukan percakapan yang lebih lama.
c. Mencuri Kredensial Login: Penyerang dapat menggunakan manipulasi psikologis untuk membujuk seseorang untuk memberikan nama, frasa, atau jenis login kredensial lainnya untuk akun mahal.

Berikut ini adalah beberapa opsi yang perlu dipertimbangkan untuk melindungi diri Anda dari phishing manipulasi psikologis:

a. Pertahankan Kewaspadaan: Perhatikan pesan, panggilan, atau objek lain yang mungkin mengungkapkan informasi sensitif, serta kata-kata atau tindakan apa pun yang mungkin melakukannya.
b. Verifikasi Identitas: Setelah menerima panggilan, permintaan, atau surat dari seseorang yang meminta akses ke sistem atau informasi sensitif, identitas individu diverifikasi secara pribadi melalui saluran komunikasi yang otentik.

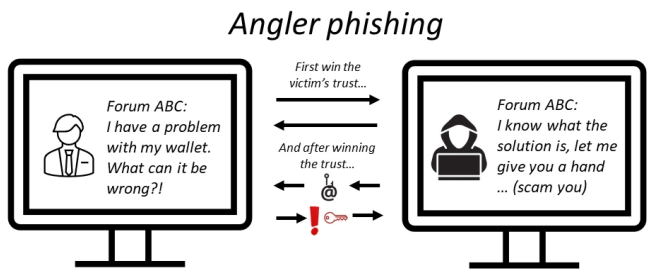
c. Keamanan Informasi: Jangan memberikan informasi pribadi atau akses ke sistem kepada siapa pun sampai Anda yakin akan identitas dan keberadaan mereka.

d. Pendidikan: Tingkatkan kesadaran Anda tentang teknik rekayasa sosial seperti phishing dan metode rekayasa sosial lainnya sehingga Anda dapat melihat potensi bendera merah dan menghindarinya.

e. Gunakan Keamanan Berlapis: Terapkan langkah-langkah keamanan seperti mengaktifkan otentikasi dua faktor, using perangkat lunak keamanan yang terpercaya, dalam melindungi serangan phishing.

Dengan berhati-hati dan mengadopsi praktik keamanan yang baik, Anda dapat melindungi diri dari serangan phishing manipulasi psikologis yang membahayakan privasi dan keamanan Anda.

14. Angler Phishing



Source: https://cdn.publish0x.com/prod/fs/cachedimages/2953651786-78eeeba26704897a0f2ecfa7f4842541cfbc6abc65bef329fc964144605c62d1.webp

Angler phishing adalah jenis phishing yang menggunakan teknik penipuan dan persuasi untuk mengelabui korban. Dalam situasi ini, tujuannya adalah untuk meyakinkan korban bahwa mereka terlibat dalam interaksi yang sah dengan pihak berwenang untuk melindungi informasi sensitif atau sistem yang tidak berfungsi.

Angler phishing sering dilakukan menggunakan situs web atau aplikasi seluler yang meniru tampilan dan fungsionalitas situs web atau aplikasi terpercaya. Penyerang membuat tautan yang menarik atau mengarahkan pengguna ke situs online palsu melalui email, pesan teks, media sosial, atau saluran komunikasi lainnya.

Situs web yang digunakan dalam phishing pemancing sering menyertakan konten yang sangat mirip dengan situs web asli. Mereka dapat menggunakan konten, desain, dan logo yang identik dengan yang ada di situs eksternal. Korban dilarang memasukkan informasi pribadi apapun, seperti nama pengguna, frasa rahasia, informasi keuangan, atau informasi pribadi lainnya.

Teknik angler phishing juga dapat menghambat penggunaan teknik pengalihan, yang secara otomatis mentransfer pengguna dari satu situs web ke situs web lain tanpa sepengetahuan mereka. Ini dilakukan dengan memanfaatkan fitur keamanan di situs web asing, atau dengan menggunakan iklan atau ejekan yang dimodifikasi.

Untuk melindungi diri Anda dari phishing pemancing, berikut ini adalah beberapa opsi yang perlu dipertimbangkan:

a. URL yang diamati: Periksa URL yang tepat dari situs web yang baru saja Anda masukkan. Asumsikan bahwa itu

adalah URL asli yang cocok dengan situs web yang harus Anda kunjungi. Perbedaan kecil dalam plot atau karakter yang mengkhawatirkan.

b. Jangan Klik Tautan Tidak Terpercaya: Hindari mengklik tautan yang dikirimkan kepada Anda melalui email, pesan teks, atau media sosial dan berasal dari domain yang tidak dikenal atau jahat. Lebih baik memasukkan URL secara manual atau menggunakan bookmark yang ada.

c. Jika Anda yakin situs web yang Anda lihat itu asli, Anda dapat mengonfirmasinya dengan menghubungi organisasi di belakangnya melalui jalur komunikasi yang aman atau dengan mengunjungi layanan komunikasi terpercaya.

d. Selamat Perangkat Lunak: Pastikan untuk memperbarui semua perangkat lunak Anda, termasuk browser web dan sistem operasi Anda, ke versi terbaru yang memiliki patch keamanan terbaru.

e. Pendidikan: Tingkatkan pemahaman Anda tentang teknik phishing dan praktik keamanan internet. Pahami berbagai jenis serangan phishing dan cara menemukannya.

Anda dapat melindungi diri dari serangan angler phishing dan menjaga privasi informasi pribadi Anda dengan menggunakan kata sandi yang kuat, URL yang dipilih dengan cermat, dan praktik terbaik lainnya untuk keamanan data.

15. Smishing Phishing

Source: https://cyberhoot.com/wp-content/uploads/2020/09/maxresdefault-5.jpg

Smishing phishing adalah jenis phishing yang melibatkan pengiriman pesan teks (SMS) atau jenis surat digital lainnya. Dalam hal ini, penyerang menggunakan tulisan yang berisiko membahayakan korban untuk membocorkan informasi pribadi atau melakukan kegiatan yang melanggar hukum.

Serangan smishing phishing sering dimulai dengan transmisi pesan teks yang singkat atau tidak ada ke audiens target. Pesan yang disebutkan di atas dapat menunjukkan bahwa itu berasal dari organisasi yang diakui, lembaga pemberi pinjaman, atau penyedia layanan. Teks dalam paragraf itu berisi prompt atau instruksi untuk mendapatkan tindakan yang relevan.

Tujuan penipuan phishing adalah untuk mendapatkan informasi pribadi seperti nomor kartu kredit, frasa rahasia, atau informasi rekening bank. Penyerang dapat menggunakan teks yang kasar secara verbal atau eksplisit secara seksual untuk segera menanggapi atau memberikan informasi yang menyesatkan.

Beberapa contoh penipuan phishing meliputi:

Pesan teks yang mengklaim bahwa akun korban mereka telah ditemukan atau terjadi kejadian yang mencurigakan dan meminta korban untuk mengklik tautan atau memasukkan kredensial login mereka untuk "memverifikasi" akun mereka.

Pesan teks yang menginformasikan bahwa korban telah memenangkan hadiah atau undian dan diminta untuk mengirimkan informasi pribadi atau melakukan pembayaran untuk mengklaim hadiah in question.

Pesan teks yang meminta izin dari klien untuk mengakses informasi kartu kredit mereka untuk membayar barang yang ditentukan atau untuk melakukan transaksi yang ditentukan.

Berikut adalah beberapa opsi yang perlu dipertimbangkan untuk melindungi diri Anda dari penipuan phishing:

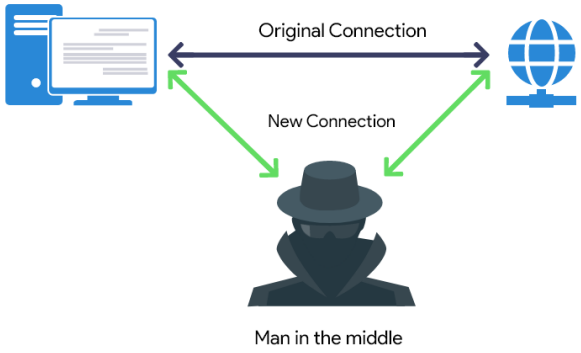
a. Pertahankan Kewaspadaan: Berhati-hatilah saat membaca konten yang mengandung konten seksual, informasi sensitif, atau materi tidak senonoh.
b. Verifikasi Identitas: Jangan langsung merespons atau mengklik tautan dalam teks yang dibatasi. Verifikasi keakuratan hasil dengan langsung menghubungkan dengan nomor terkemuka menggunakan saluran komunikasi sebelumnya yang Anda gunakan.
c. Jabatan Kerahasiaan Informasi: Kecuali Anda yakin dengan identitas dan keberadaan mereka, jangan pernah memberikan informasi pribadi atau kredensial login kepada siapapun melalui input teks.
d. Blokir atau Laporkan Pesan: Jika Anda mendapatkan tulisan yang sangat menantang, Anda dapat memblokir

nama penulis dan memberi tahu penyedia layanan Anda tentang hal ini.

e. Pendidikan: Konfirmasikan pemahaman Anda tentang jenis praktik smishing, phishing, dan peretasan etis yang terkait dengan bukti linguistik. Pahami berbagai jenis serangan phishing dan cara menemukannya.

Anda dapat melindungi diri dari serangan phishing dan menjaga privasi informasi pribadi Anda dengan mematuhi protokol keamanan seperti mengamati kewaspadaan, meninjau keaslian pesan teks, dan tidak mengungkapkan informasi sensitif kepada mereka yang tidak dapat dipercaya.

16. Man-In-The-Middle (MTM) Phishing



Source: https://beaglesecurity.com/blog/images/blogmim.png

Serangan Man-in-the-Middle (MTM) adalah serangan di mana penyerang mengintersep dan memanipulasi komunikasi antara dua pihak yang sah tanpa sepengetahuan mereka, sehingga

mereka dapat melihat, mengubah, atau mencuri informasi yang dikirimkan antara mereka.

Serangan Man-in-the-Middle biasanya melibatkan penyerang yang menggunakan celah keamanan dalam jaringan atau mengubah pengaturan perangkat atau perangkat lunak untuk mendapatkan akses ke lalu lintas data yang terus-menerus. Ini dapat terjadi melalui hotspot Wi-Fi palsu, jaringan yang tidak aman, atau serangan terhadap router atau perangkat jaringan.

Penyerang di tengah dapat melihat, merekam, atau mengubah data saat dua pihak berkomunikasi. Mereka memiliki kemampuan untuk mencuri data pribadi seperti kata sandi, nomor kartu kredit, atau informasi keuangan. Selain itu, mereka juga memiliki kemampuan untuk mengubah data yang dikirimkan untuk mencuri sesi login, mengirimkan pesan palsu, atau melakukan serangan lainnya.

Serangan Man-in-the-Middle termasuk:

a. Serangan Wi-Fi: Penyerang membuat hotspot Wi-Fi palsu dengan nama yang mirip dengan jaringan yang sebenarnya untuk menarik pengguna untuk terhubung. Ketika pengguna terhubung ke hotspot palsu, penyerang dapat mengintersep data yang dikirimkan antara pengguna dan tujuan yang dimaksud.
b. Serangan Stripping SSL: Penyerang dapat mengakses data sensitif yang seharusnya terenkripsi dengan menghilangkan lapisan keamanan SSL (Secure Sockets Layer) dalam komunikasi yang dilindungi SSL.
c. Serangan DNS Spoofing: Penyerang memanipulasi resolusi DNS (Domain Name System) untuk mengarahkan

lalu lintas ke situs web yang salah. Ini memungkinkan mereka untuk mencuri informasi login atau mengarahkan pengguna ke situs web yang berbahaya.

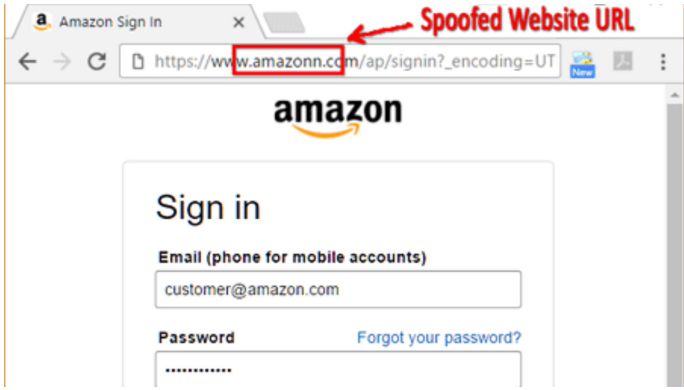
Berikut ini adalah beberapa tindakan yang dapat diambil untuk melindungi diri dari serangan Man-in-the-Middle :

a. Gunakan Koneksi yang Aman: Saat terhubung ke jaringan yang tidak dipercaya, hindari terhubung ke jaringan Wi-Fi publik yang tidak aman dan pastikan untuk menggunakan koneksi yang aman seperti VPN (Virtual Private Network).
b. Perhatikan Indikator Keamanan: Saat berkomunikasi melalui internet, perhatikan tanda-tanda keamanan seperti ikon kunci ganda atau HTTPS pada browser. Tanda-tanda ini menunjukkan bahwa koneksi dilindungi dengan enkripsi.
c. Verifikasi Identitas: Dengan memeriksa URL situs web atau layanan dengan hati-hati, Anda dapat memastikan bahwa Anda berinteraksi dengan situs web atau layanan yang sah. Selanjutnya, Anda harus mengkonfirmasi sertifikat keamanan.
d. Perbarui Perangkat Lunak: Perangkat lunak, termasuk browser web dan sistem operasi, selalu diperbarui, dengan patch keamanan terbaru.
e. Gunakan Firewall dan Keamanan Berlapis: Gunakan perangkat lunak keamanan yang dapat mendeteksi serangan Man-in-the-Middle dan melindungi lalu lintas data Anda dengan mengaktifkan firewall dan keamanan berlapis.

Anda dapat melindungi diri dari serangan Man-in-the-Middle dengan tetap waspada, menggunakan koneksi yang aman,

dan mengambil langkah-langkah keamanan yang tepat. Anda juga dapat menjaga keamanan komunikasi dan data pribadi Anda.

17. Website Spoofing Phishing



Source: https://en.wikipedia.org/wiki/File:Paypal_Phishing_Scam_Example.png

Spoofing Phishing adalah serangan di mana penyerang membuat halaman web palsu yang meniru tampilan dan fungsi dari situs web yang sebenarnya. Tujuan dari serangan ini adalah untuk menipu pengguna untuk mengunjungi situs web palsu dan memasukkan informasi pribadi mereka atau merusak sistem mereka.

Serangan website spoofing mencoba meniru situs web yang dikenal dan dipercaya, seperti situs perbankan, e-commerce, atau media sosial. Mereka mungkin menggunakan metode seperti memalsukan URL, membuat tampilan yang mirip, dan meniru elemen desain dan konten dari situs web yang sebenarnya.

Penyerang dapat mengarahkan orang ke situs web palsu dengan berbagai cara, seperti mengirim email phishing dengan tautan palsu, menggunakan iklan atau tautan yang diubah, atau memanfaatkan celah keamanan pada situs web asli untuk mengarahkan orang ke situs web palsu.

Setelah pengguna masuk ke situs web palsu, mereka mungkin diminta untuk memberikan informasi pribadi seperti nama pengguna, kata sandi, atau rincian kartu kredit. Hacker kemudian dapat menggunakan informasi ini untuk tujuan yang merugikan seperti pencurian identitas, pencurian dana, atau serangan lainnya.

Beberapa langkah yang dapat diambil untuk melindungi diri dari serangan website spoofing adalah:

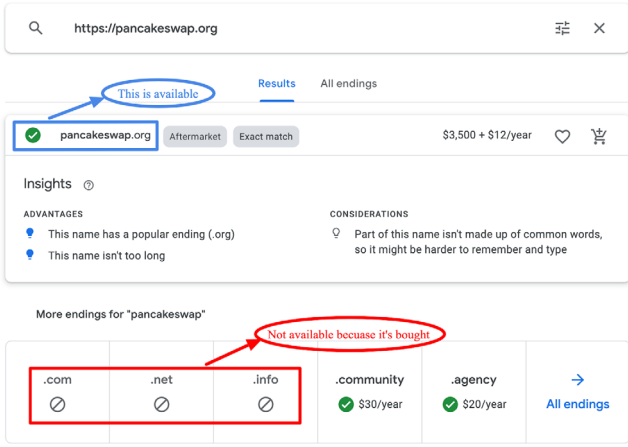
a. Periksa URL: Pastikan URL situs web yang Anda kunjungi sesuai dan valid. Waspadai perubahan kecil dalam pengejaan atau karakter.
b. Jangan Klik Tautan yang Mencurigakan: Anda harus menghindari mengklik tautan yang mencurigakan yang dikirim melalui email, pesan teks, atau media sosial. Anda lebih baik menggunakan bookmark Anda atau memasukkan URL secara manual.
c. Verifikasi Keaslian Situs Web: Jika Anda merasa bahwa situs web yang Anda kunjungi tampak mencurigakan, Anda harus menghubungi pihak berwenang secara langsung atau melalui saluran komunikasi yang terpercaya untuk memastikan bahwa itu benar.

d. Perbarui Perangkat Lunak: Perangkat lunak Anda, termasuk browser web dan sistem operasi, selalu diperbarui, dengan patch keamanan terbaru.

e. Pendidikan Pribadi: Tingkatkan pengetahuan Anda tentang serangan website spoofing dan praktik keamanan online. Pahami tanda-tanda serangan phishing dan bagaimana menghindarinya.

Dengan berhati-hati, memeriksa kredibilitas situs web, dan menghindari memberikan data pribadi Anda ke situs web yang tidak dapat dipercaya, Anda dapat melindungi diri dari serangan website yang menipu dan menjaga informasi pribadi Anda aman.

18. Domain Spoofing Phishing



Source: https://edgemesh.com/5e3d3268a134a79339be8368/6224180469ec387666da3a99_UEDEEKusR5SazhWw9CCO6uXkqdIkTWulUsMehbKtu93peHn0Gr3mPtXpFyDCzJmF8LY1ydb7JpdU3B4O8P-9hVxI98d7Qb1XtYJVG8QI8JB1f5Gnx-kLDU-oQ17VHjdkPggi-3Xl.png?em-origin=assets.website-files.com

Jenis serangan phishing yang dikenal sebagai domain spoofing adalah serangan di mana penyerang mencoba menipu pengguna dengan membuat URL situs web yang sebenarnya dengan memalsukan atau mengubah nama domain. Tujuannya adalah untuk membuat pengguna percaya bahwa mereka berinteraksi dengan situs web yang sebenarnya, padahal sebenarnya mereka berada di situs web palsu yang dikendalikan oleh penyerang.

Serangan domain spoofing phishing menggunakan metode seperti memalsukan atau mengubah nama domain situs web yang sebenarnya. Penyerang dapat menggunakan karakter yang mirip atau mengganti beberapa huruf dalam nama domain untuk memberi kesan bahwa situs web tersebut adalah versi asli. Misalnya, mereka mungkin menggunakan domain "g00gle.com" daripada domain "google.com".

Serangan phishing biasa melibatkan meminta informasi pribadi seperti kata sandi, nomor kartu kredit, atau informasi lainnya. Setelah pengguna masuk ke situs web palsu, penyerang akan mencoba mendapatkan informasi pribadi atau keuangan mereka.

Serangan domain spoofing phishing menggunakan berbagai strategi, seperti:

a. Typosquatting: Penyerang membuat domain yang mirip secara pengejaan dengan menggunakan kesalahan pengejaan umum dalam nama domain situs web yang dikenal. Misalnya, mereka dapat menggunakan alamat web "facbook.com" daripada alamat web Facebook.
b. Homograph Attacks: Penyerang dapat membuat nama domain palsu yang mirip dengan situs web asli dengan

menggunakan karakter yang sama secara visual tetapi berbeda secara Unicode. Mereka dapat menggunakan huruf Kiril atau karakter Unicode lainnya yang mirip dengan huruf Latin.

c. Subdomain Spoofing: Untuk mengecoh pengguna, penyerang membuat subdomain palsu di bawah nama domain yang sebenarnya. Misalnya, untuk menciptakan kesan situs web yang aman, mereka dapat menggunakan domain "secure.apple.com" daripada "apple.com".

Beberapa langkah yang dapat diambil untuk melindungi diri dari serangan domain spoofing phishing adalah:

a. Periksa URL dengan Hati-hati: Pastikan URL situs web yang Anda kunjungi tidak memiliki karakter yang mencurigakan, pengejaan yang salah, atau domain yang tidak familiar.

b. Tinjau Sertifikat Keamanan: Klik ikon kunci atau gembok di bilah alamat browser untuk memeriksa sertifikat keamanan situs web. Pastikan sertifikat tersebut valid dan dikeluarkan oleh otoritas sertifikasi terpercaya.

c. Gunakan Bookmark atau Tautan yang Terpercaya: Untuk mengakses situs web yang sah, gunakan bookmark atau tautan yang sudah dikenal dan dapat diandalkan. Hindari mengklik tautan yang mencurigakan yang dikirim melalui email atau pesan teks.

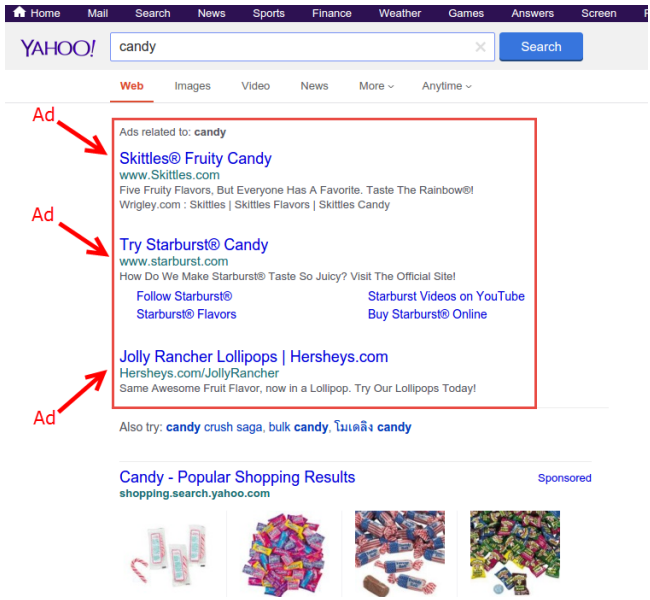
d. Verifikasi Identitas: Jika Anda merasa ada sesuatu yang mencurigakan, Anda harus menghubungi pihak berwenang secara langsung atau melalui saluran komunikasi yang

terpercaya untuk memastikan bahwa situs web tersebut adalah asli.

e. Gunakan Perlindungan Keamanan yang Tepat: Aktifkan perangkat lunak keamanan seperti firewall, perangkat lunak antivirus, dan perangkat lunak anti-phishing yang dapat membantu mengidentifikasi situs web palsu atau mencurigakan.

Anda dapat melindungi diri Anda dari serangan domain spoofing phishing dan menjaga keamanan data pribadi Anda saat menggunakan internet dengan mengambil langkah-langkah keamanan yang tepat.

19. Search Engine Phishing



Source: https://kratikal.com/blog/wp-content/uploads/2021/04/Search-Engine-Phishing-Attack-Example.png

Serangan phishing Search Engine adalah jenis serangan di mana penyerang mencoba menipu pengguna dengan mengubah hasil pencarian mesin pencari seperti Google, Bing, atau Yahoo. Tujuan utama serangan ini adalah untuk mengarahkan pengguna ke situs web palsu yang meniru situs web yang sebenarnya dengan tujuan mendapatkan informasi pribadi atau merusak sistem pengguna.

Dalam serangan phishing search engine, penyerang akan mencoba mengubah hasil pencarian agar situs web palsu mereka muncul di antara hasil yang relevan dan sah. Mereka dapat melakukan ini dengan menggunakan metode seperti mengubah metadata, mengoptimalkan kata kunci palsu, atau menggunakan teknik SEO *(Search Engine Optimization)* yang tidak etis untuk meningkatkan peringkat situs web palsu tersebut.

Ketika orang mengklik tautan yang muncul dalam hasil pencarian, mereka akan diarahkan ke situs web palsu yang meniru situs web yang sah. Situs web palsu biasanya memiliki desain, desain, dan logo yang sangat mirip dengan situs web asli. Tujuannya adalah untuk memaksa pengguna untuk memberikan data pribadi seperti nama pengguna, kata sandi, atau informasi kartu kredit.

Beberapa tindakan yang dapat dilakukan untuk melindungi diri dari serangan phishing search engine adalah:

a. Periksa URL dengan Hati-hati: Saat Anda mengklik tautan dalam hasil pencarian, pastikan URL tersebut adalah URL yang sah dan relevan dengan situs web yang Anda tuju.
b. Tinjau Deskripsi dan Sumber: Jika deskripsi singkat yang muncul dalam hasil pencarian terdengar mencurigakan

atau sumbernya tidak diketahui, lebih baik hindari mengklik tautan tersebut.

c. Perbarui Browser dan Keamanan Sistem: Pastikan browser web dan sistem operasi Anda selalu tersedia dalam versi terbaru, yang memiliki patch keamanan terbaru.

d. Gunakan Perlindungan Keamanan yang Tepat: Aktifkan fitur keamanan perangkat lunak antivirus atau keamanan internet Anda untuk mengidentifikasi situs web palsu atau berbahaya.

e. Pendidikan Diri: Tingkatkan pengetahuan Anda tentang serangan phishing dan praktik keamanan online. Pelajari tanda-tanda serangan phishing dan bagaimana menghindarinya.

Anda dapat melindungi diri dari serangan phishing search engine dan menjaga keamanan saat menggunakan mesin pencari dengan tetap waspada dan menggunakan langkah-langkah keamanan yang tepat.

TEKNIK MANIPULASI SOSIAL YANG DILAKUKAN OLEH PELAKU

Salah satu komponen penting dari serangan phishing adalah teknik manipulasi sosial, yang digunakan oleh penyerang phishing untuk memanipulasi korbannya untuk memberikan informasi sensitif atau melakukan tindakan yang merugikan. Berikut ini adalah beberapa teknik manipulasi sosial yang sering digunakan oleh penyerang phishing:

1. Penipuan Identitas, juga dikenal sebagai spoofing: Penyerang phising sering menggunakan metode spoofing untuk menyamarkan atau memalsukan identitas mereka. Mereka dapat menipu alamat email, nama pengirim, atau header email sehingga terlihat seolah-olah pesan tersebut berasal dari sumber yang terpercaya, seperti bank atau perusahaan terkemuka.
2. Tekanan Waktu (Urgency): Penyerang phising seringkali membuat korbannya tertekan dengan mengirimkan pesan yang menekankan urgensi. Untuk membuat korban panik dan mengabaikan peringatan, mereka menggunakan kata-kata seperti "tindakan segera diperlukan" atau "akun Anda akan dinonaktifkan."

3. Sosial Rekayasa (Social Engineering): Penyerang phising menggunakan sosial rekayasa sebagai teknik manipulasi psikologis untuk memanipulasi korbannya. Untuk mendapatkan kepercayaan korban dan meminta informasi pribadi atau rahasia, mereka dapat berpura-pura menjadi anggota tim dukungan pelanggan, mitra bisnis, atau teman yang dikenal.
4. Manipulasi Emosi: Penyerang phising sering mencoba mengendalikan perasaan korban untuk mendapatkan reaksi yang diinginkan. Mereka dapat memaksa korban untuk melakukan tindakan yang diminta, seperti mengklik tautan berbahaya atau membuka lampiran berbahaya, dengan menggunakan ancaman, kerentanan emosional, atau imbalan palsu.
5. Pemalsuan Situs Web (Pharming): Pembajakan atau pemalsuan situs web yang sah adalah teknik phising yang dikenal sebagai "pharming." Dengan mengarahkan korbannya ke situs web palsu yang terlihat seperti situs web asli, penyerang berusaha mencuri data masuk atau membuat korban mengungkapkan informasi pribadi.
6. Pengalihan Perhatian (Distraction): Penyerang phising dapat menggunakan teknik pengalihan perhatian untuk mengalihkan perhatian korban dari tanda-tanda peringatan. Ini dapat mencakup informasi atau penawaran yang menarik untuk membuat korban fokus pada hal tersebut daripada mengabaikan ketidaksesuaian atau kejanggalan lainnya.
7. Pretexting: Teknik manipulasi sosial di mana penyerang phishing membuat skenario atau alasan yang tidak masuk akal untuk mendapatkan informasi dari korban. Untuk meyakinkan korban bahwa mereka membutuhkan informasi pribadi atau

akses ke akun korban, mereka dapat mengaku sebagai anggota tim internal perusahaan, penyedia layanan, atau pihak otoritas.

8. Penggunaan Logos atau Tampilan Merek Palsu: Penyerang phishing sering menggunakan logo, ikon, atau tampilan merek palsu dalam pesan atau situs web mereka untuk memberi kesan bahwa mereka adalah asli, sehingga pengguna dapat mengenali merek tersebut dan memberikan informasi tanpa mencurigai bahwa pesan atau situs web tersebut adalah asli.
9. Teknik Persuasif: Penyerang phishing menggunakan taktik persuasif yang kuat untuk meyakinkan korban untuk mengikuti instruksi yang diminta. Mereka dapat menggunakan imbalan palsu, penawaran menarik, atau janji hadiah untuk menarik korban untuk memberikan informasi sensitif atau melakukan tindakan tertentu.
10. Phishing Melalui Media Sosial: Penyerang phishing juga menggunakan media sosial untuk melakukan serangan mereka. Mereka dapat membuat akun palsu atau mencuri akun yang sudah ada untuk mempengaruhi dan memanipulasi pengguna media sosial. Memposting tautan berbahaya di profil atau grup atau mengirim pesan pribadi yang tampak asli adalah beberapa contoh teknik ini.

A. DAMPAK DAN KERUGIAN DARI PHISHING

Jika seseorang terkena serangan phishing, dampak dan kerugian yang dialami korban tidak akan main-main baik bagi perseorangan maupun bagi organisasi. Yakni :

1. Kehilangan Data Pribadi: Serangan phishing dapat menyebabkan seseorang atau organisasi kehilangan informasi pribadi sensitif seperti nomor rekening bank, nomor kartu

kredit, atau informasi identitas lainnya. Penyerang dapat menggunakan data ini untuk melakukan pencurian identitas, kegiatan keuangan yang merugikan, atau penipuan lainnya.

2. Keuangan: Phishing dapat mengakibatkan kerugian besar bagi individu dan organisasi. Jika seseorang memiliki akses ke informasi keuangan, penyerang dapat melakukan transaksi ilegal atau mencuri dana dari rekening bank. Organisasi juga dapat menghadapi biaya pemulihan, kerugian uang karena pelanggaran data, dan reputasi yang buruk yang dapat mempengaruhi kepercayaan pelanggan.
3. Penurunan Reputasi: Serangan phishing dapat merusak reputasi perusahaan. Organisasi yang tidak melindungi data pelanggan dan mitra bisnis mungkin kehilangan kepercayaan mereka, yang dapat menyebabkan penurunan pendapatan, kehilangan pelanggan, dan kesulitan membangun kembali kepercayaan.
4. Gangguan Operasional: Serangan phishing dapat mengganggu operasi individu maupun organisasi. Serangan yang berhasil dapat mengunci akun, menghentikan akses ke sistem atau layanan penting, dan mengganggu produktivitas. Selain itu, saat perusahaan berusaha untuk melindungi data dan memulihkan sistem, mereka dapat mengalami downtime yang signifikan.
5. Serangan Lebih Lanjut: Serangan phishing yang berhasil dapat memicu serangan seperti malware, ransomware, atau serangan jaringan lainnya. Penyerang dapat menggunakan informasi yang mereka peroleh dari serangan phishing untuk merencanakan serangan yang lebih kompleks.

Dengan itu, beberapa statistik dan contoh kasus nyata tentang kerugian yang terjadi akibat serangan phishing, sebagai berikut :

1. Laporan Investigasi Data Breach 2021 Verizon menyatakan bahwa 36% dari serangan phishing yang dilaporkan melibatkan penipuan credential, yang dapat menyebabkan kerugian data keuangan dan pribadi yang signifikan.

   Sumber: Laporan Investigasi Data Breach 2021 oleh Verizon, yang dapat diakses di https://enterprise.verizon.com/resources/reports/dbir/.

2. Laporan Anti-Phishing Working Group (APWG) pada kuartal keempat tahun 2020 menunjukkan peningkatan signifikan dari 225.304 situs web phishing yang dilaporkan dibandingkan kuartal sebelumnya.

   Sumber: Laporan Tingkat Aktivitas Phishing Q4 2020 APWG (https://docs.apwg.org/reports/apwg_trends_report_q4_2020.pdf).

3. Laporan Phishing Activity Trends dari APWG pada tahun 2020 menunjukkan bahwa institusi keuangan adalah sasaran paling sering dari serangan phishing, dengan 25,5% dari semua serangan tersebut ditujukan pada mereka.

   Sumber: APWG, "Phishing Activity Trends Report 2020" (https://docs.apwg.org/reports/apwg_trends_report_2020.pdf).

Dengan contoh kasus nyata :

1. Serangan Phishing pada Google dan Facebook: Pada tahun 2017, seorang penipu dari Lithuania berhasil melakukan serangan phishing yang canggih untuk menggelapkan lebih dari $100 juta dari perusahaan teknologi Google dan Facebook. Penipu

itu menggunakan email dan dokumen palsu untuk mengirim faktur palsu ke kedua perusahaan.
Sumber: Artikel BBC News berjudul "Pria bersalah atas penipuan $100 juta terhadap Google dan Facebook"
(https://www.bbc.com/news/technology-48725620).

2. Serangan Phishing pada Formulir W-2: Pada tahun 2016, serangan phishing yang ditargetkan pada karyawan perusahaan teknologi Seagate mengakibatkan pencurian lebih dari 10.000 formulir W-2, yang dikenal sebagai formulir pajak karyawan. Data pribadi pekerja, seperti nama, alamat, nomor jaminan sosial, dan informasi keuangan lainnya, dapat bocor sebagai hasil dari serangan hacker.

   Sumber: "Phishers Spoof CEO, Request W-2 Forms" dari KrebsOnSecurity (https://krebsonsecurity.com/2016/03/phishers-spoof-ceo-request-w2-forms/).

3. Serangan Phishing pada Equifax: Pada tahun 2017, perusahaan kredit Equifax menjadi korban serangan phishing yang mengakibatkan kebocoran data pribadi sekitar 147 juta pelanggan. Penyerang berhasil mendapatkan akses ke sistem Equifax melalui email phishing palsu yang dikirimkan ke karyawan.

   Sumber: "Equifax Data Breach Settlement", yang dapat diakses di Federal Trade Commission (FTC) di sini:

   https://www.ftc.gov/enforcement/cases-proceedings/refunds/equifax-data-breach-settlement.

B. PENCEGAHAN DAN PERLINDUNGAN DARI SERANGAN PHISHING

Dengan adanya serangan phishing membuat semua masyarakat resah dan harus berhati-hati lagi. Berikut tips pencegahan dan perlindungan dari serangan phishing yang bisa kami berikan agar anda, keluarga, dan organisasi anda tetap aman.

1. Kesadaran Pengguna:
    a. Tingkatkan kesadaran pengguna tentang serangan phishing, seperti cara membedakan email, pesan, atau situs web yang mencurigakan.
    b. Pelajari pengguna tentang cara menjaga keamanan online, seperti menghindari mengklik tautan atau lampiran yang mencurigakan, memberikan login atau data pribadi secara sembarangan, dan tidak berbagi data pribadi melalui email atau pesan yang tidak terenkripsi.
2. Pendidikan dan Pelatihan:
    a. Berikan pelatihan rutin kepada karyawan tentang serangan phishing dan strategi yang digunakan oleh penyerang. Simulasikan serangan dengan alat pelatihan yang memungkinkan karyawan untuk mengenali dan melaporkan serangan tersebut. Berikan panduan yang jelas tentang tindakan yang harus diambil jika seseorang mencurigai serangan phishing.
3. Verifikasi identitas Anda:
    a. Sebelum memberikan informasi sensitif, pastikan Anda mengetahui siapa orang yang memintanya melalui email, pesan, atau telepon.

b. Untuk melindungi akun online Anda, gunakan metode otentikasi kuat seperti verifikasi dua faktor (2FA).

4. Penyeleksi email:
   a. Gunakan program keamanan email yang dapat mengidentifikasi dan memfilter email phishing sebelum mencapai kotak masuk pengguna.
   b. Perbaiki sistem perlindungan email secara berkala.
5. Keamanan dan Pembaruan Perangkat Lunak:
   a. Selalu memperbarui perangkat lunak sistem operasi, browser web, aplikasi, dan program keamanan dengan patch keamanan terbaru.
   b. Aktifkan fitur pembaruan otomatis untuk memastikan perangkat selalu memiliki perlindungan terbaru.
6. Antivirus dan firewall:
   a. Untuk melindungi sistem dari serangan phishing dan malware, aktifkan dan perbarui firewall dan program antivirus.
7. Lihat situs web:
   a. Sebelum memberikan data pribadi atau melakukan transaksi online, pastikan situs web aman. Ini dapat dilihat dengan melihat tanda ikatan keamanan dan tanda kunci keamanan pada alamat URL (https://).

Modul ini membahas serangan phishing, efeknya, dan cara mencegahnya. Serangan phishing merupakan ancaman besar bagi individu dan organisasi, dengan potensi kehilangan uang, data pribadi, dan reputasi. Namun, dengan meningkatkan kesadaran pengguna, pelatihan keamanan, penggunaan teknologi deteksi dan

filtering yang canggih, dan pentingnya pembaruan perangkat lunak, kita dapat mengurangi risiko dan melindungi diri kita dari serangan phishing.

Penting untuk selalu waspada dan mengambil tindakan keamanan yang diperlukan dalam kehidupan digital kita. Selalu verifikasi siapa pihak yang meminta data pribadi kita, hindari mengklik tautan atau lampiran yang mencurigakan, dan gunakan hanya saluran yang aman dan terpercaya untuk memberikan login atau informasi pribadi kita. Untuk melindungi diri kita sendiri, juga penting untuk mengikuti pelatihan keamanan dan melaporkan serangan phishing yang terdeteksi.

Ingatlah bahwa serangan phishing terus berkembang, jadi penting untuk selalu tahu tentang cara baru yang digunakan oleh penyerang. Dengan menjaga keamanan digital kita, kita dapat menjaga privasi, melindungi keuangan kita, dan mengurangi risiko serangan phishing.

Untuk memastikan bahwa pengalaman online kita aman dan aman, mari kita prioritaskan kesadaran digital dan keamanan digital.

REFERENSI

https://www.fortinet.com/resources/cyberglossary/types-of-phishing-attacks

https://www.researchgate.net/publication/279270088_An_Introduction_to_Digital_Crimes

https://threatcop.com/blog/how-are-phishing-attacks-successful/#:~:text=Lack%20of%20awareness,falling%20victim%20to%20 phishing%20 attacks.

Kumar, A., Srivastava, A., & Chandra, A. (2018). Machine learning based phishing detection: A review. Computers & Security, 77, 219-246.

Almukaynizi, M., Abdullah, A. B., & Bhatti, Z. A. (2016). Phishing detection techniques: A review and analysis. Computers & Security, 59, 226-257.

Sheng, S., Holbrook, M., & Kumaraguru, P. (2010). Phishing and countermeasures: understanding the increasing problem of electronic identity theft. IEEE Security & Privacy, 8(6), 42-49.

Jakobsson, M., & Myers, S. (2007). Phishing and countermeasures: A taxonomy of anti-phishing methods. In Proceedings of the 2007 ACM workshop on Digital identity management (pp. 1-10). ACM.

Dhamija, R., Tygar, J. D., & Hearst, M. (2006). Why phishing works. In Proceedings of the SIGCHI conference on Human Factors in computing systems (pp. 581-590). ACM.

Hadnagy, C. (2011). Social engineering: The art of human hacking. John Wiley & Sons.

Anti-Phishing Working Group (APWG) - www.antiphishing.org

Phishing.org - www.phishing.org

United States Computer Emergency Readiness Team (US-CERT) - www.us-cert.gov

Federal Trade Commission (FTC) - www.ftc.gov

The United States Department of Homeland Security - www.dhs.gov

Kaspersky - www.kaspersky.com

Cybersecurity and Infrastructure Security Agency (CISA) - www.cisa.gov

Symantec - www.symantec.com

The National Cybersecurity and Communications Integration Center (NCCIC) - www.us-cert.gov

WASPADA

KEJAHATAN *PHISHING ATTACK!*

Menurut organisasi internasional APWG, tren kejahatan online Phishing terus meningkat dari tahun ke tahun. APWG mengukur tren serangan phishing dari banyaknya jumlah situs phishing unik yang dikirimkan melalui e-mail secara global. Datanya berasal dari laporan mitra-mitra riset APWG di berbagai negara, serta dari aduan publik yang dilaporkan langsung ke situs APWG.

Menurut laporannya, APWG menemukan jumlah serangan phishing pada tahun 2022 naik jauh dibanding tahun-tahun sebelumnya. Sepanjang 2019, jumlah serangan yang dilaporkan masih di bawah 100 ribu situs phishing unik per bulan. Kemudian pada 2020-2021 jumlahnya mencapai kisaran 200 ribu situs per bulan, dan melonjak lagi ke kisaran 300 ribu-400 ribu situs per bulan hingga mencapai rekor tertinggi pada Desember 2022.

Phishing adalah salah satu metode penipuan online yang paling umum dan berbahaya pada tahap personal. Menurut laporan Data Breach Investigations Report di tahun 2019 oleh Verizon di Amerika Serikat, phishing merupakan penyebab tertinggi kebocoran data (32%). Phishing bertujuan untuk mencuri data pribadi atau keuangan korban dengan cara mengirimkan pesan atau mengarahkan korban ke situs web palsu yang meniru situs resmi. Dampak dari phishing bisa sangat merugikan bagi korban, baik secara finansial maupun psikologis.

Klinik Digital
Member of

Penerbit litnus.
literasinusantaraofficial@gmail.com
www.penerbitlitnus.co.id
@litnuspenerbit
literasinusantara_
085755971589

Teknologi +17
ISBN 978-623-114-655-7
9 786231 146557