DIGITAL PROTECTION OF PRIVATE INFORMATION

Orang-orang di era modern tidak bisa lepas dari internet dan perangkat elektronik. Selain itu, orang saat ini berlomba-lomba untuk memperluas akun jejaring sosial mereka untuk menjadi populer seperti Facebook, Twitter, Instagram, Snapchat, dan masih banyak lagi. Orang-orang di seluruh dunia juga dapat mengakses berbagai artikel melalui situs web dan jejaring sosial untuk mendapatkan berita terbaru. Untuk mengakses berbagai jejaring sosial ini, seharusnya orang menggunakan browser web. Semua orang pasti memiliki akun jejaring sosial. Selain itu, lahan berbisnis seperti toko online juga menggunakan sosial media. Kegiatan ini mudah dan menguntungkan karena tidak membutuhkan modal dan hanya perlu memposting produk yang dijual. Anda dapat membayar dengan rekening, COD, market, dan lain-lain.

Dengan meningkatnya jumlah pengguna sosial media di seluruh dunia, penjahat siber di seluruh dunia mulai melakukan tindakan mereka untuk mengambil keuntungan dari pengguna sosial media. Salah satunya adalah phishing, yang merupakan bentuk tindakan mengancam atau menjebak seseorang dengan gagasan memancing mereka. Dengan kata lain, menipu seseorang sehingga dia secara tidak langsung memberikan semua informasi yang dibutuhkan penjebak. Phishing adalah salah satu jenis kejahatan siber yang sekarang marak terjadi. Tindakan kriminal juga semakin merebak di seluruh dunia seiring berjalannya waktu. Karena itu, ancaman yang sangat besar saat ini juga terjadi melalui internet. Cara ini merupakan cara paling mudah untuk dijadikan serangan oleh para hacker. Meskipun tampak sederhana, masih ada pengguna yang masuk ke perangkap sang hacker.

Kami telah melakukan survei literatur tentang phishing dan membaca beberapa jurnal untuk mengetahui sumber ancaman phishing. Berikut adalah garis besar dari beberapa sumber ancaman phishing yang telah kami temukan:  
 1. Email

Serangan ini dimulai dengan email yang tampaknya berasal dari organisasi yang dekat dengan korban. Setelah itu, email akan meminta mereka untuk memperbarui data mereka dengan mengikuti link URL yang tercantum dalam email tersebut. Phishing pada dasarnya menggunakan vektor serangan kompleks dan rekayasa sosial untuk membuat ilusi atau penipuan di mata penerima email. Penyerang akan mengirimkan jutaan email ke jutaan pengguna, dan setidaknya ribuan dari mereka akan tertipu oleh rekayasa tersebut. Serangan-serangan ini pasti menggunakan email palsu untuk menipu pengguna untuk membocorkan data pribadi.

2. Website

Mereka akan diminta untuk memberikan informasi pribadi seperti password dan nomor rekening bank di situs web, yang pada akhirnya akan digunakan untuk pencuri identitas. Selain itu, phiser menggunakan alat untuk mencuri kode sumber dari situs web resmi dan menggantinya dengan situs web palsu. Selain itu, phiser membuat embedding link untuk mendapatkan informasi pribadi korban.

3.Malware

Metode penyerangannya dengan berpura-pura meminta korban untuk men-download file phiser sebagai penetralisir malware di komputernya.

Dari definisi phishing, Anda dapat melihat bagaimana pekerjaan phishing dilakukan untuk memancing korban ke dalam jebakan phisher. Phishing adalah aktivitas seseorang untuk mendapatkan informasi sensitif pengguna menggunakan email dan situs web palsu yang terlihat seperti tampilan dan nuansa asli atau resmi dari situs web yang sebenarnya. Phisher menggunakan email, spanduk, atau pop-up untuk mengelabui pengguna agar dialihkan ke halaman web palsu tempat pengguna diminta memberikan informasi pribadi. Di sinilah para phisher memanfaatkan ketidakpedulian dan ketidakpedulian pengguna jaringan palsu untuk mendapatkan informasi. Berikut ini adalah aspek dari ancaman yang terinfeksi oleh virus phishing:

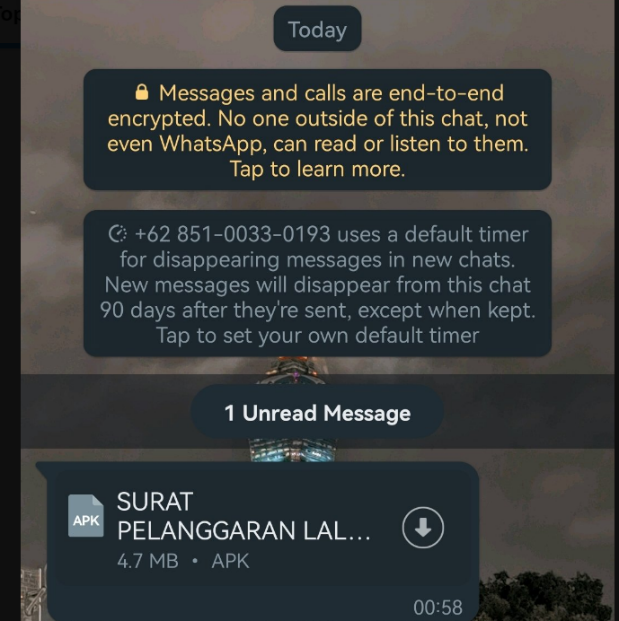
1. Manipulasi Tautan: Beberapa teknik phishing menggunakan manipulasi tautan untuk membuat alamat web institusi aslinya terlihat seperti yang sebenarnya. Penyusup sering menggunakan URL yang salah atau subdomain. Salah satu contohnya adalah URL berikut: www.micosoft.com [www.mircosoft.comwww.microsoft.com](http://www.mircosoft.comwww.microsoft.com)

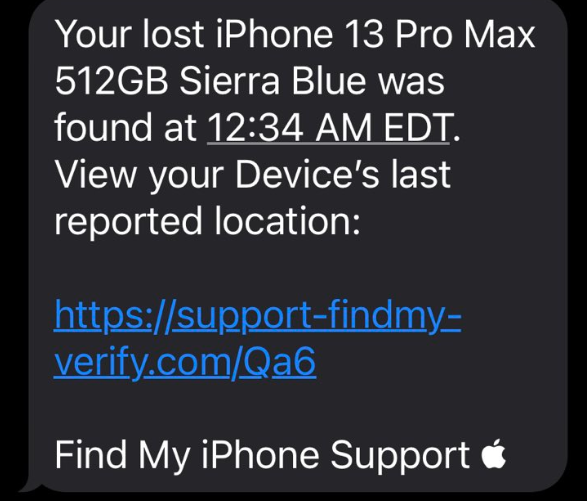
2. Filter Evasion Phisher memaksa orang untuk mengungkapkan data pribadi mereka dengan menggunakan gambar daripada teks. Akibatnya, baik Gmail maupun Yahoo secara default menonaktifkan gambar untuk email masuk. Phisher/penipu memposting:

a. Tautan yang mengarah ke halaman web yang sah tetapi sebenarnya mengarah ke halaman web phishing untuk membuat email phishing terlihat lebih asli.   
  
b. Mungkin juga munculan yang persis sama dengan halaman resminya

Berikut contoh-contoh link phising yang sering dijumpai:







Reference:

K. S. Adewole, N. B. Anuar, A. Kamsin, K. D. Varathan, and S. A. Razak, “Malicious accounts: Dark of the social networks,” J. Netw. Comput. Appl., vol. 79, pp. 41–67, 2017, doi: <https://doi.org/10.1016/j.jnca.2016.11.030>

M. Junger, L. Montoya, and F.-J. Overink, “Priming and warnings are not effective to prevent social engineering attacks,” Comput. Human Behav., vol. 66, pp. 75–87, 2017, doi: <https://doi.org/10.1016/j.chb.2016.09.012>

N. Abdelhamid, “Multi-label rules for phishing classification,” Appl. Comput. Informatics, vol. 11, no. 1, pp. 29–46, 2015, doi: 10.1016/j.aci.2014.07.002

R. S. Rao and S. T. Ali, “PhishShield: A Desktop Application to Detect Phishing Webpages through Heuristic Approach,” Procedia