JURIKOM (Jurnal Riset Komputer), Vol. 7 No. 4, Agustus 2020
e-ISSN 2715-7393 (Media Online), p-ISSN 2407-389X (Media Cetak)
DOI 10.30865/jurikom.v7i4.2304
Hal 511-516

Analisa Mobile Phishing Dengan Incident Response Plan dan Incident Handling

Wenceslaus Candraditya Pamungkas[*], Fahmy Trimuti Saputra

Fakultas Ilmu Komputer, Program Studi Teknik Komputer, Universitas Amikom Yogyakarta, Sleman, Indonesia.
Email: [1,*]Wenceslaus.pamungkas@students.amikom.ac.id, [2]Fahmy.s@students.amikom.ac.id
Submitted 29-06-2020; Accepted 16-08-2020; Published 31-08-2020

Abstrak

Tindakan kejahatan yang terjadi pada jaman modern ini semakin berkembang dan bermacam-macam, kejahatan yang terjadi saat ini juga sudah merambah kedunia maya, yang berupa kejahatan Phising, dimana korban akan dimintai informasi pribadi yang berkedok menggunakan web palsu yang sengaja disebar melalui jejaring sosial seperti email, chatting, broadcast, dll. Kejahatan ini akan memanfaatkan data dan informasi yang di dapatkan untuk melakukan tindak kejahatan yang dimana sang korban tanpa sadar menginputkan data pribadi mereka ke dalam web pancingan yang sengaja disiapkan dan disebar, dimana data dan informasi tersebut menjadi salah satu akses untuk masuk ke dalam layanan yang korban miliki. Dengan menggunakan metode Incident Respon Plan (IRP) dan Incident Handling yang dimana membantu seseorang dalam melakukan perlindungan terhadap data pribadi yang dimiliki oleh setiap individu dan dimana kita sebagai pengguna selayaknya untuk dapat melindungi data dan informasi diri yang dimana menjadi akses untuk masuk kedalam layanan. Dengan IRP dan Incident Handling seseorang akan mengetahui hal apa saja yang dapat dilakukan untuk melindungi setiap informasi yang ada, mulai dari persiapan sebelum terkena serangan phising ataupun jika kita sudah terkena serangan Phising.

Kata Kunci: Mobile Phishing, Incident Response Plan, Informasi, Internet, Forensik

Abstract

Acts of crimes that occur in modern times are growing and varying, crimes that occur at this time have also penetrated cyberspace, in the form of phishing crimes, where victims will be asked for personal information under the guise of using fake websites intentionally spread through social networks such as email, chat, broadcast, etc. This crime will use the data and information obtained to commit a crime in which the victim unconsciously enters their personal data into a web trick that is deliberately prepared and disseminated, where the data and information becomes one of the accesses to enter into the victim's services have. By using the Incident Response Plan (IRP) and Incident Handling methods which help someone in protecting the personal data owned by each individual and where we as users should be able to protect the data and personal information which becomes accessible to enter the service. With IRP and Incident Handling, someone will know what can be done to protect any information, from preparation before a phishing attack or if we have been hit by a phishing attack.

Keywords: Mobile Phishing, Incident Response Plan, Information, Internet, Forensic

1. PENDAHULUAN

Saat ini, kehidupan masyarakat kebanyakan bergantung pada gadget ataupun smartphone dan paket data atau koneksi internet, ini menjadikan sebuah celah dimana orang-orang yang tidak bertanggung jawab memanfaatkan lalu lintas jaringan yang padat dan banyak, sehingga dapat muncul tindak kejahatan yang mungkin saja mengincar banyak orang diluar sana melalui berbagai macam jenis media sosial yang mereka gunakan, diantaranya adalah phising

Pengertian phising sendiri dalam dunia keamanan komputer adalah aktivitas kriminal yang dimana seseorang dengan sengaja ingin mendapatkan informasi pribadi yang valid dengan menggunakan teknik yang tidak sah[1], atau dengan kata lain kita menyebutnya sebagai pencurian data, dengan memanfaatkan website tiruan yang diinputkan dalam sebuah link yang sengaja disebar melalui jejaring sosial maupun WAG yang saat ini sedang marak, diharapkan dari pesan broadcast tersebut ada yang akan tertarik untuk mengunjungi website tersebut.

Dikutip dari lembaga Pew Research Center yang merupakan salah satu lembaga peneliti di amerika serikat menerbitkan laporan tentang Negara dengan orang dewasa terbanyak yang menggunakan smartphone, laporan ini diterbitkan pada tahun 2019, dimana Indonesia berada pada peringkat ke enam Negara berkembang dengan pengguna smartphone terbanyak, dimana 42 % memiliki smartphone, 28% memiliki HP biasa, dan 29% tidak memiliki HP, itu membuktikan bahwa lalu lintas penggunaan smartphone di kalangan orang dewasa cukup tinggi.

Dengan adanya lalu lintas tersebut, bukan tidak mungkin tindak kejahatan yang ada di dunia maya juga akan menyerang para pengguna, yang marak pada masa ini adalah broadcast tentang pemberian kuota maupun hadiah gratis yang diberikan oleh brand atau provider yang ada. Oleh karena itu dengan adanya karya tulis ini diharapkan banyak orang akan lebih berhati-hati dan tau apa yang harus di lakukan dengan data informasi pribadi yang menyangkut pada identitas, dimana identitas biasanya digunakan untuk mencari sosial media, akun m-banking, dan lain-lain yang dapat merugikan diri kita sendiri. Dengan menggunakan protokol yang baik sebagai pencegahan dan penanggulangan yang tepat. Tujuan dari penulisan studi kasus ini adalah untuk memberikan edukasi pada pengguna smartphone dengan kemungkinan terjadinya tindak kejahatan phising[2], dan bagaimana cara menanggulangi sesuai dengan Incident Respon Plan maupun Incident Handling. Manfaat dari penulisan adalah untuk mendapatkan cara terbaik dari Incident Respond dan Incident Handling terkait serangan phising yang ada pada smatphone. Sehingga dapat meminimalisir tindak kejahatan yang ada, serta meningkatkan kewaspadaan setiap pengguna smartphone terkait pesan berantai yang sering diterima dari berbagai sumber yang tidak bisa dipertanggung jawabkan kredibilitasnya.

2. METODE PENELITIAN

JURIKOM (Jurnal Riset Komputer), Vol. 7 No. 4, Agustus 2020
e-ISSN 2715-7393 (Media Online), p-ISSN 2407-389X (Media Cetak)
DOI 10.30865/jurikom.v7i4.2304
Hal 511-516

Pengertian dari Phising adalah tindakan kriminal untuk mencuri informasi pribadi orang lain menggunakan entitas elektronik dimana salah satu caranya adalah dengan website, pada sebuah website dikategorikan sebagai website phising apabila memiliki karakteristik seperti address bar based feature, abnormal based feature, HTML and javascript based feature, dan domain based feature (Mohammad, McCluskey, & Thabtah, An Assessment of Features Related to Phising Website using an Autimated Technique, 2012)[3]. Dari pengertian tersebut, metode yang saat ini marak digunakan adalah dengan melakukan penyebaran tautan yang dimana didalamnya terdapat website phising yang sudah otomatis terbuka bila kita mengklik tautan tersebut, kita akan masuk ke dalam sebuah website phising yang sengaja dibuat menyerupai website asli, ini merupakan ciri khusus yang dimiliki teknik phising untuk menjebak para korbannya.

Informasi yang diharapkan oleh Phisher adalah berupa data pribadi yang dapat digunakan sebagai bahan untuk menemukan media sosial, akun banking[4], email, yang berhubungan langusung dengan smartphone anda, dimana saat ini sebagian besar orang akan mengaktifkan aplikasi yang menggunakan basic login menggunakan email, kata sandi, dan akan saling terhubung satu dengan yang lain, seperti ovo yang dapat terkoneksi langsung dengan grab dan tokopedia, yang akan menjadi celah dimana bila satu akun bisa diretas dari data dan informasi yang dikumpulkan berdasarkan tindak kejahatan phising ini, akun dan yang ada di dalam smartphone kita bisa tertakedown oleh orang yang tidak bertanggung jawab.

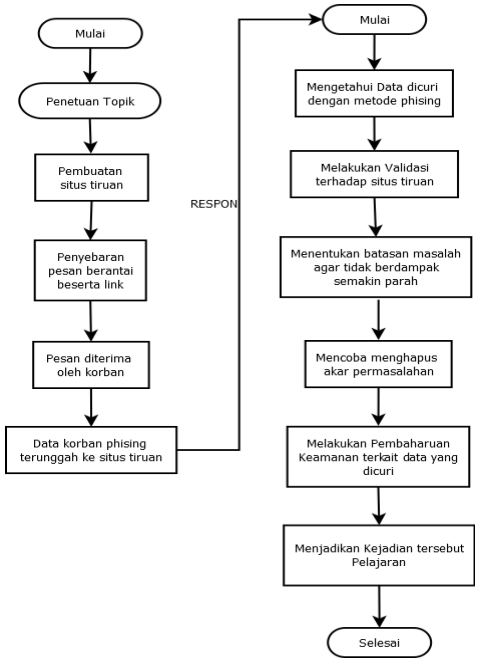
Maka dari itu pada studi kasus ini kami mencoba mengumpulkan informasi yang didapat dari Whatsapp Grup kemudian kita lakukan scanning dengan menggunakan laman virus total yang digunakan untuk melakukan analisa singkat terkait website yang ada, selain itu dari virus total nantinya juga akan didapatkan graph yang dimana akan menunjukkan relation yang dimiliki dari masing-masing parental website tersebut, mulai dari url, hingga mengarah pada apa saja yang ada pada website tersebut.

3. HASIL DAN PEMBAHASAN

Perkembangan dari berbagai macam serangan didunia maya saat ini menjadi sangat pesat dan semakin luas, serta makin banyaknya pengguna smartphone yang juga secara otomatis terkoneksi dengan internet, namun tidak diimbangi dengan tingkat pemahaman yang cukup untuk memilah dan memilih informasi maupun kegiatan bahkan tindakan kejahatan yang bisa terjadi melalui dunia maya dengan bermodalkan jejaring sosial yang saat ini melekat pada setiap orang[5].

Selain itu dengan berkembangnya teknologi menjadikan tindak kejahatan yang tadinya dilakukan secara langsung melalui serangan beruba wujud nyata terhadap barang atau benda yang ada, kini serangan tindak kejahatan dapat dilakukan dengan metode jarak jauh dengan memanfaatkan media internet, guna mengumpulkan informasi target secara mendetail, salah satu cara yang digunakan adalah teknik phising,

Saat ini phising sudah merambah dunia mobile, terutama saat masa pandemic covid – 19 yang menyerang berbagai macam Negara maupun sektor ekonomi membuat beberapa oknum memanfaatkannya guna melakukan tindak kejahatan dunia maya berupa phising[6], yang disebarkan melalui jejaring sosial salah satunya adalah aplikasi whatsapp, dimana pada fitur whatsapp terdapat group chat dimana didalamnya terdapat lebih dari satu orang dalam satu ruang obrolan yang sama, pesan berantai yang berisi ajakan untuk mendapatkan hadiah secara gratis menjadikan beberapa orang mengunjungi tautan tersebut[7] dan setelah kami lakukan analisa sederhana didapatkan sebuah informasi bahwa didalam tautan tersebut mengandung unsur phising dan Trojan, berikut kami berikan skema berupa flowchart yang dimana dapat menjadi alur serangan yang terstruktur.



Gambar 1. Skema alur serangan yang terstruktur

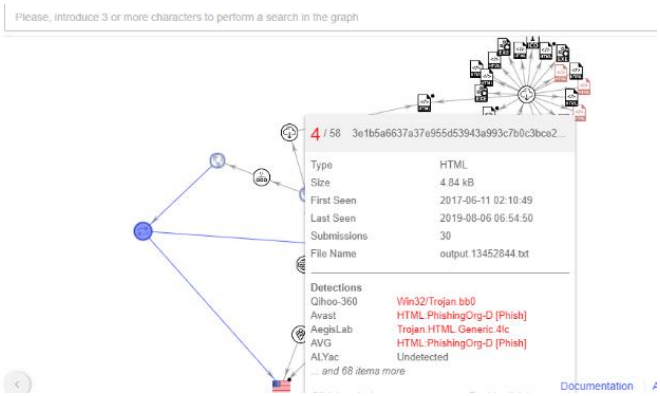
JURIKOM (Jurnal Riset Komputer), Vol. 7 No. 4, Agustus 2020
e-ISSN 2715-7393 (Media Online), p-ISSN 2407-389X (Media Cetak)
DOI 10.30865/jurikom.v7i4.2304
Hal 511-516

Pada gambar flowchart tersebut digambarkan bahwa proses dari tindak kejahatan phising yang di susun guna menjerat korban agar dapat percaya, tindakan ini bertujuan untuk mengelabuhi target dengan menggunakan iklan maupun ajakan guna melakukan klik terhadap tautan yang disebar melalui situs jejaring sosial, dimana pada situs yang dibuat tersebut sengaja dibuat mirip dengan website yang asli, sehingga dapat meningkatkan keyakinan bahwa pesan berantai tersebut memang benar adanya[8]

Kemudian beberapa bukti sebaran yang didapatkan terkait sebaran broadcast hoax yang mengandung phising yang kami temukan dibeberapa WAG, yang nantinya akan kami analisa dengan sederhana menggunakan virus total.

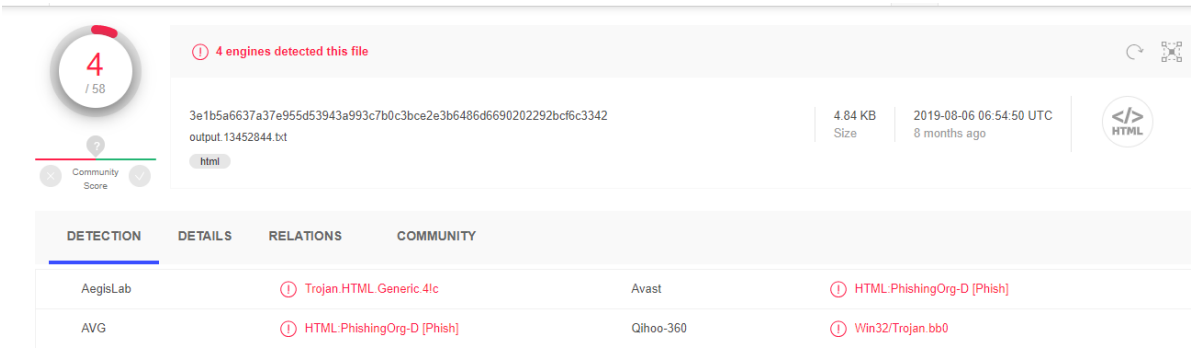
Gambar 2. Sebaran broadcast hoax

Bahkan dari kedua grup tersebut yang tidak memiliki sangkut paut bisa mendapatkan broadcast yang sama dengan url https://whatscoupon.club/id-20gb dimana dari hasil yang didapat setelah dilakukan pemetaan dari url tersebut didapatkan bahwa terindikasi sebagai web phising yang terekam pada virus total.



Gambar 3. Web phising yang terekam

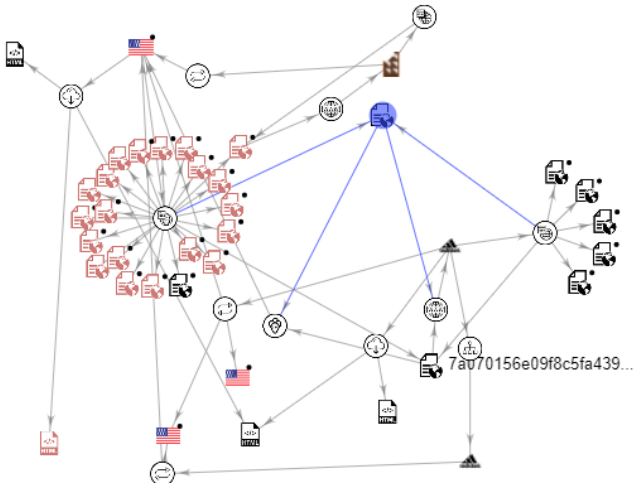
Selain itu juga didapatkan sejenis wintrojan yang juga terdapat didalam url tersebut, ini dapat membahayakan keamanan dari sebuah informasi yang ada pada sebuah smartphone yang mana pada setiap smartphone biasanya terhubung ke berbagai macam aplikasi yang berhubungan langsung dengan database, ataupun aplikasi yang dapat mengakses data pribadi seperti nomer telefon, pesan, atau bahkan galeri pada smartphone.



Gambar 4. Url webphising yang terekam

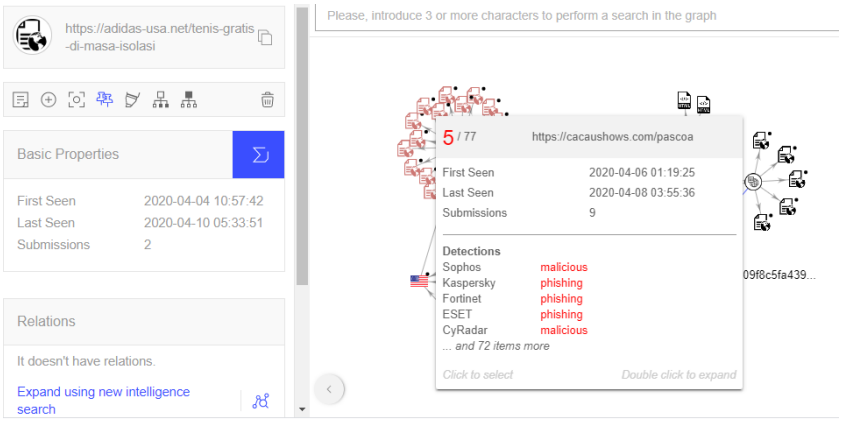
Selain url yang ada di atas, juga ada url yang lain yang juga disebar melalui jejaring sosial whatsapp, dengan url https://adidas-usa.net/tenis-gratis-di-masa-isolasi, dari url tersebut ditawarkan berupa hadiah terhadap siapapun yang mau mendapatkan sepatu dengan merk dan brand ternama, dengan mengunjungi tautan tersebut.

JURIKOM (Jurnal Riset Komputer), Vol. 7 No. 4, Agustus 2020
e-ISSN 2715-7393 (Media Online), p-ISSN 2407-389X (Media Cetak)
DOI 10.30865/jurikom.v7i4.2304
Hal 511-516



Gambar 5. Network sebaran web phising

Dari gambar pengamatan diatas ini jelas terlihat memang ada logo dimana menunjukkan tiruan dari website asli dari merk brand ternama tersebut, namung dibagian lain terdapat indikasi phising yang ditemukan pada informasi dari virus total seperti pada gambar dibawah ini.



Gambar 6. Properti web phising

Dengan ditemukannya fakta bahwa url yang disebarkan tersebut mengandung unsur phising yang dapat di tumpangi dengan malware yang dapat menyerang smartphone menjadikan kewaspadaan dari setiap user selaku pengguna dari smartphone agar lebih cermat dan jeli dalam memilih dan memilah informasi maupun tautan yang diterima dari sumber yang tidak diketahui kredibitasnya. Hendaknya waspada terkait tindakan phising berdasarkan point-poin yang sudah kami coba kumpulkan sehingga dapat menjaga kita sebagai user dalam melakukan aktifitas dunia maya dan data pribadi kita tetap aman dari tindak kejahatan yang ada didunia maya. Tindakan perencanaan ini dilakukan untung menghadapi masalah keamanan dari data yang mana sering kita sebut dengan istilah IRP (Incident Respon Plan)[9] dimana poin-poin dari IRP itu sendiri adalah sebagai berikut :

a. Preparation

Pada fase ini, kita sebagai *user* hendaknya mengetahui bahwa kita memiliki data dan informasi pribadi yang tidak semua orang dapat mengakses secara bebas, untuk lebih tepatnya mengarah pada privasi diri kita sendiri mengenai data dan informasi yang hendaknya kita jaga dan menjadikan kita lebih waspada, apabila mendapatkan sebaran pesan atau informasi yang meminta kita untuk melakukan pengisian informasi pribadi di dunia maya yang tidak dapat kita jamin tingkat keamanan dari data yang diberikan. Selain itu juga kita hendaknya mengerti akan data pribadi kita yang hendak digunakan untuk keperluan apa saja, sehingga kita sebagai pengguna bisa melakukan *pengawasan* yang berkala dan membuat data kita yang ada di Bank, Kantor, atau apapun itu menjadi aman dan dipastikan tidak digunakan oleh orang yang tidak berkepentingan.

b. Identification

Terkadang data pribadi yang kita miliki yang mungkin menjadi salah satu alat akses ke berbagai kepentingan bisa kita berikan secara percuma, mengakibatkan munculnya berbagai kejanggalan yang mungkin saja kita sebagai *user* tidak merasakan dampaknya secara langusng namun dikemudian hari dapat merugikan diri sendiri. Sebagai orang yang hidup di dunia serba modern dan serba online hendaknya kita mengetahui bahwa data pribadi kita hanya kita berikan kepada mereka yang berhak, jika mendapatkan informasi yang tidak kita ketahui masuk melalui email, chatting, SMS, atau apapun itu yang berbentuk digital, hendaknya kita memvalidasi informasi tersebut agar apa yang kita lakukan tidak menuju kepada kesalahan yang fatal dikemudian hari. Jika mendapatkan Pesan dari pihak yang tidak kita ketahui

kejelasannya yang menginstruksikan bahwasanya kita harus melakukan validasi ulang melalui halaman web atau apapun itu yang menuntun kita untuk memberi data pribadi, hendaknya kita waspada bahwa tindakan tersebut termasuk kedalam tindak kejahatan PISHING yang sering marak terjadi di dunia maya, yang mencari kelalian *user* dalam menjaga data pribadinya.

c. Containment & Escalation

Melakukan pembatasan insiden yang terjadi menjadi sangat penting saat kita sudah menyadari bahwa kita terkena jebakan PISHING yang dimana orang yang tidak kita kenal mempunyai informasi pribadi kita yang setiap saat bisa saja digunakan utuk tindak kejahatan yang dapat merugikan diri kita sendiri, walaupun yang menyebabkannya juga diri kita sendiri.

Melakukan pemetaan terhadap data pribadi kita menjadi sangat penting, karena dengan kita mengetahui dengan jelas data pribadi kita digunakan untuk kepentingan apa saja, kita bisa melakukan pembatasan masalah agar tidak merembet ke masalah yang lebih besar dan tidak semakin merugikan diri kita sendiri.

Yang dimana data pribadi biasanya berhubungan dengan tempat bekerja, bank, social media, dll yang pada setiap bagian tersebut memiliki tingkat kerugiannya masing-masing apabila data dan informasi pribadi kita digunakan secara tidak bijak, maka dari itu hendaknya kita melakukan pemetaan terhadap kegunaan dari data pribadi kita masing-masing.

d. Eradication

Setelah kita mengetahui dari masalah yang sedang kita alami yaitu PISHING, yang kita lakukan selanjutnya adalah menghapus akar permasalahan tersebut. Menghapus akar permasalahan ini dengan maksud kita melakukan penanggulangan yang seharusnya kita lakukan untuk mengurangi, melindungi, dan membatasi agar data tersebut tidak semakin tersebar luas dan mengakibatkan kerugian karena digunakan untuk kepentingan yang tidak sesuai dengan apa yang kita kehendaki.

e. Recovery

Melakukan *recovery* atau pembaharuan adalah salah satu cara terampuh untuk menanggulangi kejahatan PISHING selain dengan melaporkan ke Lembaga yang terkait apabila ada penggunaan data informasi pribadi. Karena data yang ada adalah data pribadi maka akibat dari penyalahgunaan data tersebut akan berimbas pada satu individu yang akan bertanggung jawab atas data yang ada dan menjadikannya sasaran tindak kejahatan dunia maya yang mungkin saja mengintai setiap orang yang dengan tanpa sadar memberikan infomasi data pribadi ke orang lain. Pembaharuan ini yang dimaksud adalah dengan melakukan update, pengaturan ulang terhadap semua layanan yang dimana data informasi digunakan untuk menjadi *akses* yang sangat vital, dengan membaharui dan mengatur ulang semua layanan, setidaknya mengurangi akibat dari ketidak waspadaan kita yang dapat merugikan diri kita dari segi *finansial*, *nama baik*, *dll* yang dimana mungkin akan menjadi momok yang sangat membebani apabila data dan informasi tersebut benar-benar digunakan untuk hal yang tidak bertanggung jawab.

f. Lessons Learned

Manusia di jaman sekarang dengan segala kecanggihan yang ada di dunia, dengan segala dampaknya yang tanpa kita sadari kita akan cepat atau lambat masuk ke dalam fasenya teknologi modern. Dampak yang ada tak selamanya baik, juga tak semuanya buruk. Kita sebagai *user* hendaknya lebih cerdas untuk memilih dimana kita akan berpijak dan dimana kita akan menancapkan paku kehidupan ini. Tindak kejahatan pada jaman seperti saat ini tidak selalu dalam bentuk kekerasan fisik, namun dengan perkembangan teknologi kejahatan dunia maya terkadang lebih kejam dan lebih terasa menyakitkan karena di dunia maya tersebut seluruh dunia bisa mengetahui apa yang terjadi di belahan dunia lain dalam hitungan menit bahkan detik. Kita sebagai manusia yang menggunakan teknologi secara baijak, hendaknya melakukan *upgrade* terhadap wawasan di dunia luar yang menjadikan kita semakin terlindungi dan bisa mengurangi kerugian dan membantu mencegah orang lain yang belum mengerti tentang bahaya kejahatan dunia maya agar tidak semakin banyak yang menjadi korban diluar sana, karena pada intinya Pengalaman adalah guru terbaik, dan jadikan pengalaman sebagai media belajar yang menjadikan kita lebih baik untk kedepannya.

Maka dari itu diperlukannya tindakan pencegahan maupun penanggulangan yang tepat terkait mobile phising yang saat ini marak terjadi, dimana kita dapat melakukan tindakan berdasarkan Incident Respon Plan ataupun Incident Handling yang bisa diterapkan dalam melakukan penanggulangan tindak kejahatan phising yang sedang terjadi.

Setelah tau tentang IRP pada pembahasan berikutnya akan di ulas tentang incident handling, dimana pada incident handling merupakan sebuah kegiatan yang bertujuan untuk meerapkan IRP yang sudah dirancang bila terjadi serangan terhadap sistem maupun kebocoran data, sehingga guna meminimalisir informasi yang bocor[10] akibat tindakan phising bisa kita lakukan dengan :

a. Melakukan tracking terhadap data dan informasi yang dicuri.
b. Mengamankan aplikasi yang berhubungan langsung dengan perbankan atau virtual monay.
c. Melakukan reset password pada semua akun yang terkoneksi dengan data yang diberikan.
d. Melaporkan secepatnya pada call center terkait data dan informasi yang mungkin saja bocor dan disalahgunakan oleh orang lain.
e. Melakukan pembersihan device yang digunakan terkait Log, history, cookie, dll.
f. Mengaktifkan otentikasi ganda dan jangan memberikan kode otentikasi kepada siapapun.

Dengan langkah-langkah diatas setidaknya kita bisa melakukan penanggulangan yang mempersulit phiser dalam menggunakan data dan informasi pribadi kita untuk tindak kejahatan ataupun untuk diperjual belikan.

Tindakan kejahatan phising yang terjadi ini dapat dikategorikan pada pelanggaran UU ITE dimana diatur dalam undang terkait jaminan keamanan warga negara dalam menggunakan akses telekomunikasi, pasal-pasal yang bisa dijadikan pedoman adalah :

1. konten ilegal, yang terdiri dari, antara lain: kesusilaan, perjudian, penghinaan/pencemaran nama baik, pengancaman dan pemerasan (Pasal 27, Pasal 28, dan Pasal 29 UU ITE)
2. Akses ilegal (Pasal 30)
3. Itersepsi ilegal (Pasal 31)
4. Gangguan terhadap data (data interference, Pasal 32 UU ITE)
5. Gangguan terhadap sistem (system interference, Pasal 33 UU ITE)
6. Penyalahgunaan alat dan perangkat (misuse of device, Pasal 34 UU ITE)

4. KESIMPULAN

Dari pembahasan yang ada dapat disimpulkan bahwa seringnya kita sebagai user tidak memperhatikan keamanan data dan informasi pribadi kita, dan juga kita terkadang tidak bisa memilah dengan baik informasi yang diterima di media sosial, dimana pada kenyataanya kita tidak dapat tau kredibilitas dari informasi ataupun tautan yang beredar luas. Maka dari itu dari hasil pembahasan didapatkan cara yang tepat dan efisien dalam menangani tindak kejahatan phising yang sudah merambah ke dunia smartphone dengan melalui sebaran tautan yang sangat masif, serta dengan menggunakan IRP dan incident handling kita sebagai user menjadi lebih berhati-hati serta waspada dalam setiap menentukan langkah saat menggunakan media sosial. Serta dengan tidak menyebarkan informasi yang didapatkan kita dapat membantu untuk tidak menjerumuskan orang lain dalam tindak kejahatan phising yang sering mewabah saat ini, dengan mencari sumber informasi yang valid seperti mengunjungi situs resmi, ataupun menelfon call center terkait himbauan atau berita yang didapatkan, sehingga tidak semakin banyak orang yang termakan oleh tindak kejahatan dunia maya seperti saat ini.

REFERENCES

[1] D. Rachmawati, "Phising Sebagai Salah Satu Bentuk Ancaman Dalam Dunia Cyber," *J. Ilm. Saintikom, Univ. Sumatera Utara, Medan*, vol. 1978–6603, pp. 209–216, 2014.
[2] I. Radiansyah and Y. Priyadi, "Analisis Ancaman Phishing Dalam," vol. 7, no. 1, 2016.
[3] B. M. Susanto, "Identifikasi Website Phising Dengan Seleksi Atribut Berbasis Korelasi," *Semin. Nas. Teknol. Inf. dan Komun. 2016*, vol. 2016, no. Sentika, pp. 18–19, 2016.
[4] O. Indra, B. Trisno, and M. Kom, "Phishing Crime," pp. 108–110, 2009.
[5] R. Hakimi, "Jurnal Pustakawan Indonesia Volume 11 No. 2 Studi Isu Keamanan Jaringan Pada Facebook Rifqy Hakimi 1 1," vol. 11, no. 2, pp. 1–14.
[6] Z. Efendy, I. E. Putra, and R. Saputra, "Asset Rental Information System and Web-Based Facilities At Andalas University," *J. Terap. Teknol. Inf.*, vol. 2, no. 2, pp. 47–58, 2019, doi: 10.21460/jutei.2018.22.103.
[7] B. M. Cerda and S. Yuan, "A Study of Anti-Phising Methodologies and Phishing Detection Algorithms," no. Ciec, pp. 79–83, 2018, [Online]. Available: https://csce.ucmss.com/cr/books/2019/LFS/CSREA2019/SAM9705.pdf.
[8] V. Suganya, "A Review on Phishing Attacks and Various Anti Phishing Techniques," *Int. J. Comput. Appl.*, vol. 139, no. 1, pp. 20–23, 2016, doi: 10.5120/ijca2016909084.
[9] S. Mitropoulos, D. Patsos, and C. Douligeris, "On Incident Handling and Response: A state-of-the-art approach," *Comput. Secur.*, vol. 25, no. 5, pp. 351–370, 2006, doi: 10.1016/j.cose.2005.09.006.
[10] M. I. Cohen, D. Bilby, and G. Caronni, "Distributed forensics and incident response in the enterprise," *Digit. Investig.*, vol. 8, no. SUPPL., pp. S101–S110, 2011, doi: 10.1016/j.diin.2011.05.012.