Peluang Keamanan Password dalam Transaksi Perbankan

Dani Indra Junaedi
Program Studi Teknik Informatika
STMIK Sumedang, Jl. Angkrek Situ No. 19, Sumedang, 45323 Indonesia
email : daniindra2405@yahoo.co.id

ABSTRACT
Teknologi sudah menjadi unsur utama dalam pelayanan jasa perbankan. Setiap nasabah memiliki akun yang bisa dimanfaatkan untuk berbagai fitur layanan perbankan. Untuk mengakses akun tersebut diperlukan password yang secure supaya tidak mudah diakses oleh orang lain. Keamanan Password menjadi syarat utama dalam keamanan suatu akun perbankan dimana pembobolan rekening nasabah dapat dihindari.Teknis pembuatan password harus mengandung karakter angka, huruf (besar kecil) dan simbol supaya tidak mudah ditebak. Semakin lengkap karakter yang digunakan dan semakin banyak jumlah karakter akan membuat password semakin aman. Walaupun secara penghitungan peluang pembobolan sangat kecil, namun perilaku social engineering tetap dianggap sebagai potensi yang membahayakan bagi keamanan suatu akun. Dalam social engineering, si pelaku memanfaatkan sifat alamiah dari manusia. Hal ini diartikan bahwa betapa sifat alami manusia dapat diketahui dan dipelajari juga dimanfaatkan untuk tujuan tertentu. Kejahatan social engineering sangat membahayakan bisnis perbankan karena berpotensi menimbulkan kerugian finansial, reputasi dan hukum bagi bank dan nasabahnya melalui serangan fisik dan serangan psikologis. Dalam tulisan ini juga akan diberikan solusi bagaimana membuat suatu password dan mengelola password supaya benar-benar aman bagi pengguna.

***Kata Kunci** : Perbankan, Password, Keamanan Transaksi, Nasabah, Peluang Pembobolan*

1. Introduction

Perkembangan teknologi informasi membuat institusi perbankan mengubah strategi bisnis dengan menempatkan teknologi sebagai unsur utama dalam proses inovasi produk dan jasa. Seperti halnya pelayanan *e-banking* melalui ATM, *phone banking* dan *Internet Banking* yang merupakan bentuk dari pelayanan bank yang mengubah pelayanan transaksi manual menjadi pelayanan transaksi yang berbasis teknologi. Faktor kepercayaan dan efisiensi serta kualitas layanan menjadi alasan bagi institusi perbankan untuk selalu menata ulang bisnisnya dengan mencermati ketersediaan inovasi teknologi serta dampaknya bagi kelangsungan dan pertumbuhan bisnis.

Laporan World Economic Forum (2015) memprediksi Indonesia akan menjadi salah satu pasar digital terbesar di Asia Tenggara pada tahun 2020. Hal ini mempertegas peluang keuangan digital, diperkuat dengan kenyataan baru sekitar 36 persen orang dewasa di Indonesia yang memiliki rekening di bank atau sekitar 120 juta orang masuk dalam kategori unbanked. Asosiasi Penyelenggara Jasa Internet Indonesia (APJII) mencatat 132,7 juta orang Indonesia telah terhubung ke internet, berkat perkembangan infrastruktur dan mudahnya mendapatkan smartphone atau perangkat genggam. Angka ini naik pesat dari tahun 2014 yang hanya mencapai 88 juta orang.

Memahami potensi pemanfaatan teknologi yang demikian besar, perbankan pun melahirkan mobile dan internet banking yang terbukti efektif dalam memperluas jangkauan layanan, menyiasati tantangan geografis. Inovasi tersebut juga berhasil menciptakan efisiensi serta membuka opsi terhadap lebih banyak pilihan produk dan layanan perbankan, seiring dengan semakin digemari cara-cara pemasaran online. Mengoptimalkan perangkat genggam, nasabah dapat melakukan pembayaran, transfer dana, hingga tarik tunai dengan mudah melalui sentuhan jari.

Data OJK mengenai alat pembayaran menggunakan kartu (AMPK) sumber data OJK diakses 16 Mei 2018 adalah sebagai berikut :

Tabel 1. Jumlah APMK Beredar

Periode	2017	Tahun 2018		
	Desember	Januari	Februari	Maret
Kartu Kredit	17,244,127	17,400,189	17,438,938	17,396,248
Kartu ATM	8,815,007	8,942,236	8,978,019	9,259,043
Kartu ATM + Debet	155,663,442	158,382,554	161,055,020	163,488,079

Tabel 2. Transaksi Kartu ATM/Debet

Periode			Tahun 2018		
		Desember	Januari	Februari	Maret
Tunai	Volume	316,237,750	299,246,617	280,717,047	319,168,269
	Nominal	233,645,011	219,034,804	203,062,794	230,213,054
Belanja	Volume	50,274,051	46,596,738	39,396,293	45,581,440
	Nominal	28,143,426	25,359,248	20,260,190	22,995,777
Transfer Intrabank	Volume	116,635,942	111,486,907	103,142,715	117,047,991
	Nominal	211,397,618	206,616,946	186,522,442	211,354,920
Transfer Antarbank	Volume	46,322,326	45,281,701	42,771,061	48,434,806
	Nominal	101,323,628	87,206,133	85,445,884	98,519,689
Total	Volume	529,470,069	502,611,963	466,027,116	530,232,506
	Nominal	574,509,684	538,217,131	495,291,310	563,083,441

Keterangan : Volume dalam satuan transaksi,
Nominal dalam jutaan rupiah

Dengan semakin banyaknya pengguna internet, maka semakin banyak pula potensi kejahatan dalam dunia maya, khususnya pada sektor perbankan. Kejahatan yang biasa terjadi di sektor perbankan, antara lain :

1. *Pembobolan ATM*.
2. *Skimming*.
3. *Phising* dan *Malware*

Kata kunci atau yang dikenal sebagai “password” merupakan pendekatan keamanan yang paling lumrah dipakai. Mulai dari cara mengoperasikan ATM, internet banking, email account, dan sistem operasi. Dalam memanfaatkan akun perbankan password menjadi alat pengaman terdepan dalam melakukan berbagai akses transaksi mulai dari informasi hingga transaksi financial.

Dalam melakukan transaksi menggunakan ATM akan ada 3 alat yang terlibat yaitu mesin ATM, Kartu ATM dan password sedangkan dalam aktivitas internet banking dan mobile banking hanya dua alat yang terlibat yaitu handphone/PC/Laptop user yang sudah berisi aplikasi internet banking dan password. Dengan alat-alat yang terlibat dalam melakukan transaksi tersebut sepintas terlihat aman karena :

1. Untuk transaksi ATM, kartu ATM tidak berpindah tangan dan password hanya diketahui oleh pemilik ATM.
2. Untuk transaksi mobile banking, handphone tidak berpindah tangan dan password hanya diketahui oleh user.
3. Untuk transaksi internet banking menggunakan handphone, handphone tidak berpindah tangan dan password hanya diketahui oleh user
4. Untuk transaksi internet banking menggunakan web, user id dan password hanya diketahui oleh user.

2. Research Method

2.1. Bagaimana password tersebut bisa bocor ?

System perbankan sudah dioptimalkan untuk bisa melindungi akun nasabah. Hanya saja kelengahan nasabah dalam menjaga kerahasiaan password sering menjadi kendala. Hasil pengamatan dilapangan, banyak nasabah yang tidak menyadari akan pentingnya password dalam melindungi keamanan akun-nya.

Perlakuan terhadap pin ATM

1. Menggunakan pin ATM yang mudah ditebak. Pin ATM masih menggunakan pola 6 angka. Nasabah banyak yang masih menggunakan angka standar yang mudah ditebak seperti 123456, 111111, tanggal kelahiran seperti 240574 dan sebagainya.
2. Menuliskan pin ATM di kertas, handphone bahkan di kartu ATM itu sendiri
3. Mempercayakan pin ATM kepada pihak lain seperti anak atau anggota keluarga terdekat dengan alasan supaya mudah jika lupa dan bisa menyuruh mengambil sejumlah uang jika pemilik akun berhalangan

Perlakuan terhadap password internet banking

1. Menggunakan password yang mudah ditebak. Bank menyarankan nasabah menggunakan minimal 8 digit password dengan kombinasi angka, kombinasi huruf besar-kecil dan karakter namun nasabah sering mengabaikan dan cenderung membuat password yang mudah ditebak seperti asep1234 dan sebagainya
2. Menuliskan password di tempat yang mudah diakses oleh orang lain seperti buku, handphone dan sebagainya

Hal-hal tersebut adalah peluang bagi pelaku social engineering untuk dapat melakuakan pembobolan terhadap suatu akun. Seperti diketahui bahwa *Social engineering* berfokus pada mata rantai terlemah dalam rantai kemanan informasi-manusia[1]. Kenyataannya, hampir semua solusi informasi sangat bergantung pada manusia. Kelemahan ini bersifat universal, dan terbebas dari hardware, software, platform, jaringan, dan usia peralatan. *Social engineering* telah mencapai tingkatan tertinggi kematangan sebagai strategi dalam membobol keamanan informasi. Keamanan ini digunakan perusahaan untuk melindungi apa yang dianggap asset-aset paling penting perusahaan, termasuk informasi. Mekanisme keamanan yang terbaik pun dapat ditembus dengan *social engineering*. Untuk mengurangi resiko tersebut, bank perlu untuk melatih dan mendidik staf mereka mengenai ancaman keamanan dan bagaimana caranya mengenali serangan.

Potensi perilaku social engineering berasal dari :

1. orang terdekat seperti keluarga, saudara atau teman yang memiliki kesempatan untuk bisa menggali informasi secara leluasa
2. orang lain yang memang sudah menjadikan pemilik akun bank sebagai target sasaran kemudian menggunakan metode shoulder surfing, pretexting dan dumster diving terhadap calon korbannya.

2.2. Manajemen Password [4]

Manajemen password merupakan suatu tata cara mengelola kata kunci oleh pengguna agar fungsinya sebagai gerbang keamanan informasi dapat secara efektif berperan.

Berikut adalah beberapa hal penting yang patut untuk dimengerti dan dipertimbangkan sungguh-sungguh oleh semua pengguna password.

2.2.1. Memilih Password yang Baik

Password yang dibuat sebaiknya mudah diingat oleh pemiliknya dan pada saat yang sama sulit ditebak oleh orang lain atau mereka yang tidak berhak mengetahuinya. Untuk memilih password agar aman harus terdiri dari susunan karakter yang sulit ditebak, namun di sisi lain mudah bagi sang pemilik untuk mengingatnya.

Password yang baik disarankan memiliki sejumlah karakteristik sebagai berikut:

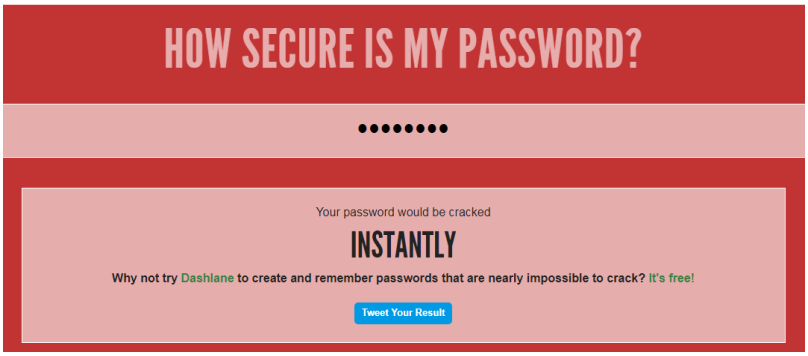
1. Terdiri dari minimum 8 karakter – dimana pada prinsipnya adalah makin banyak karakternya semakin baik, direkomendasikan password yang relatif aman jika terdiri dari 15 karakter;
2. Pergunakan campuran secara random dari berbagai jenis karakter, yaitu: huruf besar, huruf kecil, angka, dan simbol;
3. Hindari password yang terdiri dari kata yang dapat ditemukan dalam kamus bahasa atau bersifat kata umum
4. Pilih password yang dengan cara tertentu dapat mudah mengingatnya;
5. Jangan pergunakan password yang sama untuk sistem berbeda.

3. Result and Analysis

Untuk menguji seberapa aman password yang dibuat, bisa menggunakan situs dengan alamat https://howsecuremypassword.net. Melalui situs tersebut kita tinggal memasukan password untuk diuji keamanannya dalam hal ini akan diukur seberapa lama password yang dilakukan akan mampu diretas. Semakin mudah ditebak/lemah maka waktu yang dibutuhkan akan semakin singkat.

Password yang dimasukan sebanyak 8 karakter sesuai dengan jumlah minimal karakter yang diminta oleh internet banking.

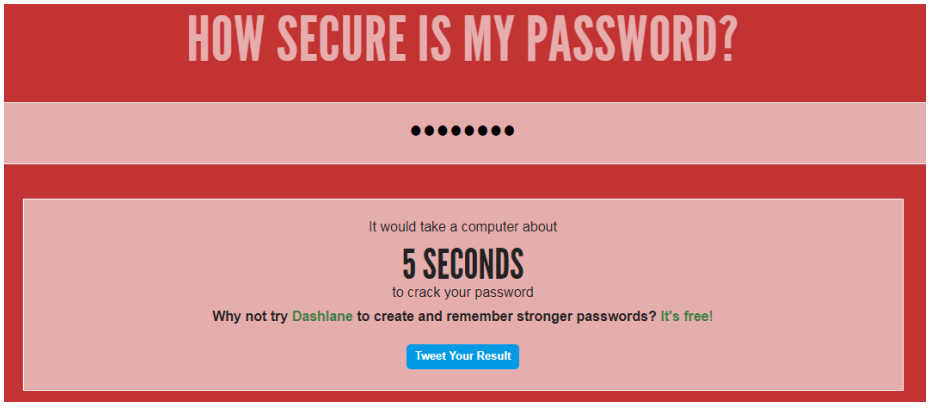
1. Password : 12345678



Gambar 1. Hasil password secara langsung

Hasilnya : password yang dimasukan dapat diretas secara langsung (instantly)

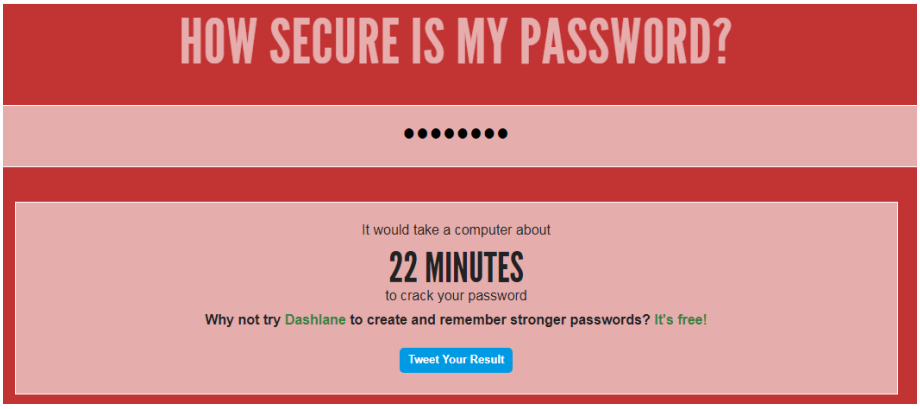
2. Password : basotahu



Gambar 2. Hasil password yang diretas

Hasilnya : password yang dimasukan dapat diretas dalam waktu singkat (5 seconds)

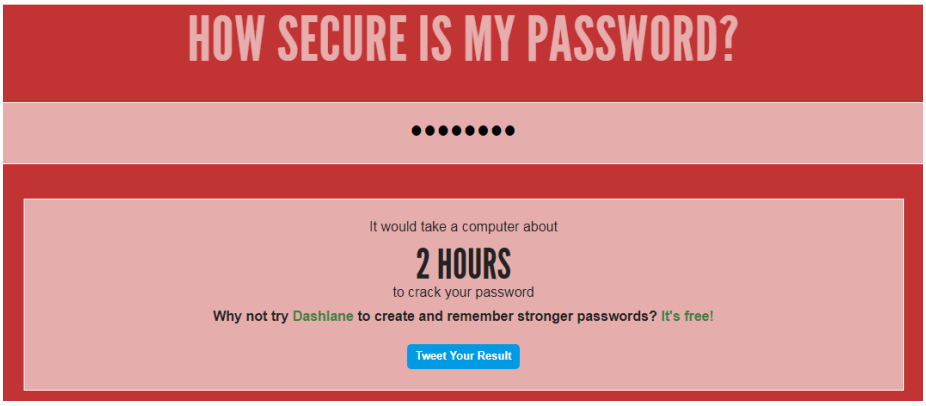
3. Password : BasoTahu



Gambar 3. Hasil password dengan kombinasi

Hasilnya : password menggunakankombinasi huruf besar dan kecil waktu. Password dapat diretas dalam waktu singkat (22 minutes) namun lebih lama daripada yang sebelumnya.

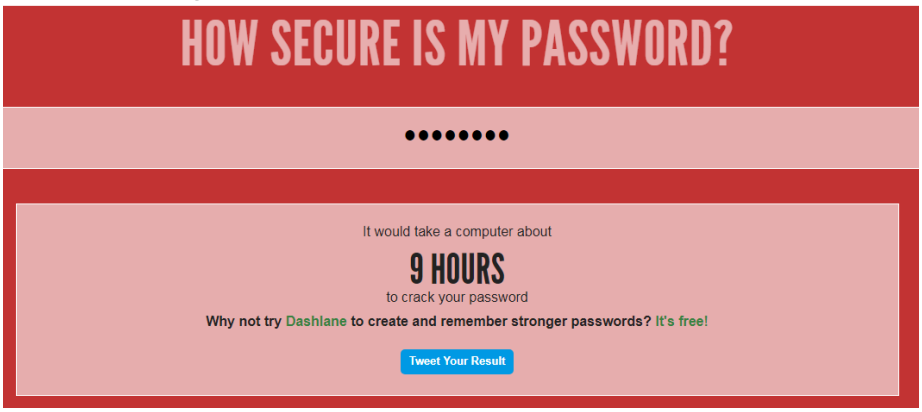
4. Password : Baso1234



Gambar 4. Hasil password dengan kombinasi angka

Hasilnya : password menggunakankombinasi angka, huruf besar dan kecil waktu, password dapat diretas dalam waktu singkat (2 hours) namun lebih lama daripada yang sebelumnya.

5. Password : Baso9@&*



Gambar 5. Hasil password dengan kombinasi angka dan karakter

Hasilnya : password menggunakan kombinasi karakter symbol, angka, huruf besar dan kecil. Password dapat diretas dalam waktu singkat (9 hours) namun lebih lama daripada yang sebelumnya.

6. Password : %"+)tA?]

Gambar 6. Hasil password dengan kombinasi angka dan karakter lain

Hasilnya : dengan menggunakan lebih banyak karakter symbol waktu yang dibutuhkan untuk meretas adalah 21 hours

7. Password : BasoTahu123/*-

Gambar 7. Hasil password dengan penambahan karakter dan kombinasi angka

Jumlah karakter password ditambah hingga 14 dengan menggabungkan angka, symbol, huruf besar dan kecil. Hasilnya password bisa diretas selama 4 billion years.

Menghitung peluang bobolnya password

1. ATM

Password/pin ATM menggunakan 6 angka dan user diberi kesempatan 3 kali memasukan pin jika pada kesempatan pertama memasukan pin salah. Berarti jika user lupa pin atau yang menggunakan bukanlah user yang berhak, hanya memiliki 3 kali kesempatan sebelum transaksi ATM di blokir. Untuk menghitung kemungkinan kombinasi 6 angka pin digunakan rumus berikut :

Notasi:

X = Jumlah karakter kombinasi

Y = Jumlah karakter password

Z = Jumlah kombinasi karakter password

$$Z = XY$$

Jumlah kombinasi pin ATM

- Karakter kombinasi adalah *hanya* angka.
- Karakter-nya yaitu: {1,2,3,4,5,6,7,8,9,0}
- Jumlah = 10
- Jumlah karakter password = 6

Maka jumlah kemungkinan kombinasi pin ATM

$Z = 10^6$

Z = 1.000.000 kombinasi

Maka peluang pin dapat dibobol adalah 1/1.000.000, jika pelaku diberikan kesempatan 3 kali oleh sistem untuk memasukan password maka peluangnya menjadi 3/1.000.000

2. Internet Banking

Karakter password internet banking lebih secure daripada pin ATM karena user diberi kebebasan menggunakan angka, huruf (besar dan kecil) dan karakter simbol dalam membuat password.

- karakter angka 10
- karakter huruf (case sensitive) 26 x 2 = 52
- karakter simbol 30
- jumlah karakter keseluruhan 92

Jika menggunakan batas minimal karakter password 8 karakter maka kemungkinan kombinasi :

$Z = 92^8$

Z = 5.132.188.731.375.620

Kemungkinan password dapat dijebol (3 kali kesempatan) yaitu 3/5.132.188.731.375.620, semakin banyak karakter password digunakan maka kemungkinan kombinasi akan semakin banyak dan peluang password bisa dijebol semakin kecil. Namun kondisi ini tidak sepenuhnya aman karena potensi yang sebenarnya adalah kelengahan user dalam menyimpan dan membuat password yang mudah ditebak. selain itu perilaku social engineering bisa menjadi potensi password yang harus diperhitungkan.

4. Conclusion

4.1. Teknis Pencegahan pembobolan Password

Berikut beberapa teknis pencegahaan pembobolan password

a. Menjaga kerahasiaan password.
   Jika seseorang menghubungi dan menanyakan password, bisa dipastikan merupakan penipuan. Selain itu jangan menyimpan informasi seperti password dengan menuliskannya dikertas dan menempelkannya di meja kerja. Jangan pernah membagi password melalui telepon pada siapapun baik yang dikenal atau tidak
b. Password timer
   Seringkali pegawai lupa melakukan proses logout dari aplikasi komputer ketika meninggalkan pekerjaan untuk suatu keperluan. Hal ini perlu diantisipasi dengan mengatur waktu aplikasi jika tidak aktif untuk logout secara otomatis sehingga kemungkinan orang lain untuk masuk ke dalam aplikasi sangat kecil karena memerlukan password untuk login kembali.
c. Karakter Password
   Dalam penggunaan password, di usahakan jangan ada sangkut paut nya dengan identitas diri kita. Karena hal tersebut sangatlah sensitif. Buatlah password yang unik dan tidak mudah di tebak oleh siapapun. kombinasi karakter di password sangat di anjurkan. dan hindari password

yang menginputkan tanggal lahir, nama panggilan, dan bersifat sensitif lainnya. Usahakan pula mengganti password baru dalam beberapa jangka waktu ke depan demi keamanan

4.2. Strategi Melindungi Keamanan Password

1. Jangan sekali-kali menyimpan password di dalam piranti elektronik seperti komputer, telepon genggam, personal digital assistant, dsb.
2. Tidak memberitahukan password anda kepada siapapun, termasuk "system administrator" dari sistem terkait;
3. Hindari tawaran fitur "save password" dalam setiap aplikasi browser atau program lainnya yang memberikan tawaran kemudahan ini;
4. Hindari memanfaatkan menu yang bisa membantu melihat password ketika sedang dimasukkan;
5. Ketika sedang memasukkan password, pastikan tidak ada orang yang berada disekitar, pastikan tidak terdapat pula kamera CCTV di belakang pundak; dan
6. Jika keadaan memaksa untuk menuliskan password di kertas sebelum memasukkannya ke dalam sistem, pastikan bahwa setelah digunakan, kertas tersebut dihancurkan sehingga tidak mungkin terbaca oleh orang lain

Password harus diganti secara berkala karena cara ini akan menyulitkan pelaku pembobolan password. Adapun cara klasik yang sering dipergunakan oleh para pembobol password adalah:

1. Menebak-nebak password dengan menggunakan analisa mengenai profil dan/atau karakteirstik pemiliknya;
2. Menggunakan "brute force attack" alias mencoba segala bentuk kemungkinan kombinasi karakter yang bisa dipergunakan dalam password;
3. Menggunakan referensi kata-kata pada kamus sebagai bahan dasar pembobolan
4. Melakukan teknik "social engineering" kepada calon korban pemilik password;
5. Melakukan pencurian terhadap aset-aset yang mengarah pada informasi penyimpanan password; dan lain sebagainya.

4.3. Beberapa metode pembuatan password menurut saran dari institusi perbankan [5]:

1. Bruce Schneier

   Metode ini diperkenalkan oleh ahli IT Security bernama Bruce Schneier pada tahun 2008. Cara kerjanya adalah : pilih sebuah kalimat dan rubahlah menjadi password. Kalimat tersebut dapat berupa apapun yang sifatnya pribadi dan berkesan untuk Anda, contohnya lirik lagu atau iklan yang dimodifikasi. Ambil beberapa huruf dari kalimat tersebut dan gabungkan, lalu tambahkan karakter – karakter spesial seperti tanda baca untuk membentuk sebuah password yang unik.
   Contoh password yang dibuat dari kalimat unik adalah :
   - Kalimat : Tolong! Bawa Aku pergi, pindah ke Wakanda
   - Menjadi password : TLG!BAp,pkWknd
   - Kalimat : Mana dimana anak kerbau paman? Oh, disana
   - Menjadi password : M?dm?akp::ohdsn4
2. Electrum

   Ide untuk metode ini berasal dari sebuah aplikasi dompet Bitcoin yang menawarkan seed 12 kata sebagai master password untuk dapat mengakses alamat – alamat Bitcoin di dalamnya. Tipe password seperti ini disebut juga dengan pass phrase, jadi daripada harus menghafal deretan karakter yang susah diingat, Anda dapat memilih frasa yang panjang. Semakin acak frasa tersebut, maka akan semakin aman
   Contoh password yang dibuat menggunakan metode ini adalah :

- Pada hari selasa kuturut kakek kedesa naik roket biasa saja kududuk dimeja
- Gelas bekas pintu lampu makan balon cangkul lari lemari tang baru buku

3. P-A-O

   Singkatan dari Person-Action-Object, metode ini dipopulerkan oleh buku berjudul Moonwalking with Einstein karangan Joshua Foer tahun 2011. Cara kerja dari metode ini adalah sebagai berikut :

   1) Pilih sebuah nama lokasi yang berkesan, contoh : Jembatan Suramadu
   2) Pilih sebuah nama figur publik yang berkesan, contoh : Elon Musk
   3) Bayangkan sebuah aktivitas unik untuk merelasikan kedua poin di atas, contoh : berperang dengan alien
   4) Lalu gabungkan ketiganya menjadi sebuah cerita singkat : "Elon Musk berperang dengan Alien di Jembatan Suramadu". Bayangan lokasi, nama, dan situasi tersebut akan mempermudah Anda untuk mengingatnya.
   5) Terakhir, ambil beberapa huruf dari cerita singkat tersebut untuk membuat sebuah password, contoh : ElMubedeAldiJS

4. Phonetic Muscle Memory

   Penemu metode ini adalah Kevan Lee, penulis artikel berjudul "Four Methods to Create a Secure Password You'll Actually Remember" di lifehacker.com. Metode ini bergantung pada fonetik (susunan huruf acak yang seolah – olah bermakna) dan kebiasaan otot tangan untuk membantu mengingat password. Cara kerja dari metode ini adalah sebagai berikut :

   1) Akses salah satu situs password generator seperti : https://identitysafe.norton.com/password-generator
   2) Buat 50 password yang minimal terdiri dari 10 karakter serta mengandung angka dan huruf besar
   3) Periksa password yang dihasilkan dan pilih yang memiliki struktur fonetik. Contohnya :
      a. drKbyn5Eta (dokter Kabayan 5 eta)
      b. P4kMudraf4N (Pak Mudrafan)
      c. caPe5uDAst0p (capek sudah stop)
   4) Ketikkan password yang telah Anda pilih di sebuah file teks dan cari mana yang gampang diketik, karena otot tangan Anda akan cepat terbiasa
   5) Simpan dan gunakan password yang fonetik dan gampang diketik tersebut

References

[1] Indrajit, R. E. Seluk Beluk Teknik Social Engineering. (http://idsirtii.or.id/cyber-6/ diakses 04 Mei 2017).
[2] Rick Nelson, "Methods of Hacking: Social Engineering," the Institute for Sistems Research, University of Maryland. (http://www.academia.edu /4903480/Methods_of Hacking-social Engineering), diakses 10 Mei 2017)
[3] How to Protect Insiders from Social Engineering Threats. (2006). (http://msdn.microsoft.com/en-us/library/cc875841.aspx, diakses 06 Mei 2017)
[4] Indrajit, R. E. Password Management. (http://idsirtii.or.id/cyber-6/ diakses 16 Mei 2018).
[5] IT Security Policy & Development Divisi PPT BRI, Password Awareness (16 Mei 2018)