# MAKALAH

# MISTERI TRANSAKSI SILUMAN REKENING JENIUS


**Disusun oleh:**

| | |
|---|---|
| Bagas Adytia Budianto | 200710888 |
| Blasius Yonas Vikariandi | 200710909 |
| Jeremi Sandy Tumanggor | 200710967 |
| Jolly Hans Frankle | 200710932 |
| Thomas Dany Haryanto | 200710947 |

**UNIVERSITAS ATMA JAYA YOGYAKARTA**


**TAHUN AKADEMIK 2020/2021**

# KATA PENGANTAR

Puji syukur kami naikkan ke hadirat Tuhan YME atas berkat dan tuntunan-Nya sehingga makalah ini dapat dikerjakan dan diselesaikan dengan baik. Makalah ini telah disusun dengan maksimal dan mendapat bantuan dari berbagai sumber, baik dari internet dan pengalaman pribadi. Untuk itu, patut kami sampaikan limpah terima kasih kepada semua pihak yang telah berkontribusi dalam pembuatan makalah ini, khususnya ibu Joanna Ardhyanti Mita Nugraha, S.Kom., M.Kom., dosen pengampu yang telah memberikan tugas ini sebagai suatu media pembelajaran Pengantar Teknik Informatika.

Makalah ini berisi penjelasan mengenai salah satu kasus *cyber crime* yang berkaitan dengan keamanan informasi, yakni kasus transaksi siluman pada rekening Jenius Bank BTPN, yang terjadi sejak pertengahan 2020 hingga saat ini. Terlepas dari semua itu, kami menyadari sepenuhnya bahwa makalah ini masih ada kekurangan dan jauh dari kata sempurna, oleh karena itu, kami meminta segala saran dan kritik dari dosen pengampu agar makalah ini dapat lebih sempurna ke depannya.

Akhir kata, kami berharap semoga makalah ini dapat memberikan manfaat dan menjadi media pembelajaran yang baik ke depannya.

Yogyakarta, 23 September 2020

Penulis

# DAFTAR ISI

# BAB I
# PENDAHULUAN

## 1.1 Latar Belakang

Seiring berjalannya waktu, dunia semakin berubah. Perubahan ini terjadi di segala bidang, baik itu bidang sosial maupun bidang sains. Salah satu perubahan tersebut terjadi di bidang siber (*cyber*) dan keamanan informasi.

Aspek keamanan informasi sangatlah dibutuhkan di dunia internet. Keamanan informasi di dunia internet tidaklah sama dengan keamanan informasi di dunia nyata. Di dunia nyata, informasi dapat diamankan dengan memegang sebuah kunci fisik. Apabila terjadi pencurian informasi, pelaku akan ditemukan di sebuah lokasi fisik. Namun hal tersebut berbeda dengan dunia internet. Dalam dunia internet, kunci untuk sebuah informasi bukan lagi sebuah kunci fisik, melainkan sebuah sistem otentikasi yang harus konfidensial, berintegritas, dan senantiasa tersedia. Namun, sistem otentikasi ini tidaklah sempurna, sehingga pencurian informasi kerap terjadi. Salah satu kasus pencurian informasi tersebut terjadi pada 2019 yang lalu, pada beberapa rekening Jenius milik Bank BTPN. Keamanan informasi merupakan sebuah hal yang wajib diwujudkan oleh setiap situs yang ada di internet, terlebih situs finansial/perbankan, yang menyimpan uang nasabah, seperti pada halnya kasus Jenius. Apa yang dilakukan oleh pihak Jenius Bank BTPN untuk mengatasi masalah ini, analisis mendalam terkait permasalahan ini, dan himbauan keamanan informasi akan dibahas lebih lanjut pada makalah ini.

## 1.2 Rumusan Masalah

1. Bagaimana kronologi transaksi siluman melalui Jenius?
2. Bagaimana analisis terhadap kasus ini?
3. Bagaimana proses penyelesaiannya?

## 1.3 Tujuan

Makalah ini bertujuan untuk memperluas pengetahuan pembaca mengenai keamanan informasi yang ada di internet, terlebih di situs finansial/perbankan. Memberi tau kepada pembaca mengenai kasus pencurian uang melalui situs finansial/perbankan sehingga pembaca bisa lebih berhati-hati supaya tidak menjadi korban dari kasus yang serupa. Memberikan pengetahuan kepada pembaca untuk mengetahui apa yang sebaiknya dilakukan jika hal tersebut terjadi kepada pembaca.

# BAB II
# PEMBAHASAN

## 2.1 Kronologi

Yang akan dibahas adalah kasus pembobolan rekening Jenius Wisnu Kumoro yang terjadi pada tahun lalu. Kronologi kejadian kurang lebih sebagai berikut:

1. Ada SMS OTP masuk, korban tidak memberikan kode *One Time Password* tersebut kepada siapapun.
2. Korban mencoba menghubungi *Customer Service* Jenius, *Customer Service* menyarankan korban untuk mengganti password.
3. Korban melanjutkan aktivitasnya dan berencana mengganti password setelah selesai.
4. Tiba-tiba muncul permintaan transaksi di Blibli.
5. Korban menghubungi *Customer Service* Jenius, saat menghubungi ternyata telah terjadi transaksi ke Blibli.
6. Saat masih menghubungi *Customer Service* Jenius korban langsung membuat pelaporan, pelaporan dicatat dan pihak Jenius menyarankan mengubah password dan email.
7. Korban mencoba mengamankan akunnya dan menghapus ponsel keduanya yang ditinggalkan di rumah.
8. Saldo Jenius korban habis.
9. Muncul SMS OTP lagi.
10. Korban tiba-tiba ter-*logout* dari aplikasi Jenius.

## 2.2 Analisis

Beberapa waktu lalu sempat heboh di sosial media beredar berita tentang *Transaksi Siluman Rekening Jenius*, dimana lebih dari satu pengguna yang terkena serangan dari anonim tersebut. Dari pihak Jenius sendiri mengatakan bahwa pelaku menggunakan modus *phising* kepada korban.

Dalam permasalahan ini, pengguna kehilangan uang yang cukup banyak hanya dalam jangka waktu yang cukup singkat. Masalah berawal saat pelaku mengirim kode OTP dan mencoba mengirim sebuah surel (*email*) kepada korban yang berisikan modus agar korban mengirim PIN mereka. Metode ini dikenal dengan sebutan *phising*, dimana pelaku mencoba berpura pura menjadi pihak Jenius agar dapat menipu korban.

Dari peristiwa tersebut korban mulai melaporkan kejadian kepada pihak Jenius, namun pihak Jenius tidak langsung menanggapi, hingga korban pun sempat membagikan kejadian tersebut ke media sosial Twitter hingga akhirnya viral dan dibaca oleh pihak Jenius sendiri. Hingga pada akhirnya, pihak Jenius menyarankan pengguna tersebut untuk memblokir kartunya, yang akan kemudian dikembalikan 14 hari kemudian. Kejadian ini termasuk cepat ditangani oleh pihak Jenius, sehingga tidak begitu banyak korban yang terkena dampak. Di bawah ini disajikan beberapa ulasan dari para *netizen* di Twitter.

1. Menurut Fanpage "*E-Commerce Shitposting*"

> kali ini kita mau bahas soal wisnu kumoro yang kemarin kebobolan akun jeniusnya
> dari kemaren banyak yg request untuk membahas
> maka kita baru bahas sekarang
> source:
> https://twitter.com/wisnuku.../status/1167081146955362306...
> cerita kronologi:
> https://www.youtube.com/watch?v=O31xL58ciCI
> karena masalah wisnu cukup unik

maka kami akan bahas teori dan analisa kami

disclaimer:

apa yang kami bahas hanya hasil analisa kami dengan berdiskusi dari beberapa narasumber yang kebetulan praktisi IT

yang terjadi sebenarnya bisa saja berbeda dari analisa kami

---

sebelumnya yang hal yang mungkin karena para pengguna jenius terbiasa mengakses jenius lewat app

sehingga banyak yang tidak tahu kalau jenius itu bisa diakses melalui web dan tidak perlu melalui aplikasi

bisa dilihat versi web jenius:

https://2secure.jenius.co.id

salah satu kemungkinan kalau log perangkat tidak tercatat melalui app

adalah akses melalui web ini

dan dari web juga dapat "remove connected device"

---

akan tetapi yang untuk kasus wisnu ini sifatnya lebih rumit daripada sekedar peretasan yang biasa tetap meminta kode OTP dari korban untuk memverifikasi transaksi tersebut

karena disini akun wisnu bisa melakukan pembelian tanpa perlu melalui otorisasi apapun dari si pemilik akun

untuk yang pernah bekerja di bagian back end e-commerce, ataupun aplikasi kekinian

pasti familiar dengan apa itu API

karena akan panjang kalau kita bahas apa itu API

mungkin untuk yang ingin tahu lebih detil bisa melihat kesini:

https://medium.com/.../how-apis-work-an-analogy-for...

biasanya via API komunikasi antar aplikasi terjadi

sehingga dalam kasus misal transaksi normal pembelian pulsa

maka:

pembeli -> pesan pulsa via blibli -> blibli menagih -> pembeli melakukan pembayaran dengan jenius -> (jenius melakukan verifikasi) -> verifikasi berhasil -

> blibli menerima pesan verifikasi pembayaran berhasil -> blibli meneruskan orderan pulsa ke operator -> operator mengirim pulsa sesuai permintaan pembeli
dalam proses ini terjadi komunikasi antara beberapa pihak
terjadinya komunikasi ini yang dilakukan via API
dan di kasus wisnu ini kemungkinan permasalahan terjadi di kasus yang kita beri kurung
(jenius melakukan verifikasi)
jika kita ibaratkan API jenius itu seperti teller bank yang mampu mengeluarkan/menyimpan uang untuk suatu keperluan
teller ini yang memeriksa kesesuaian data untuk melakukan transaksi yang dimaksud
lalu bagaimana jika kita "membajak" si teller untuk melakukan pembelian menggunakan akun orang lain
walaupun kita bukan pemilik rekening tersebut?
maka dapat terjadi seperti kasus wisnu ini
bisa dibilang kasus wisnu ini besar kemungkinan terbobol dari sisi back end API
karena si pembobol bisa melakukan "unblock" setelah si wisnu melakukan blokir terhadap semua kartu
---
TLDR:
pengguna akun jenius mengalami pembajakan akun yang melakukan pembelian di blibli tanpa verifikasi apapun
cc:
Jenius Connect
cc:
Blibli.com
cc:
Wisnu Kumoro

2. Dari Komentar "*bejo1 lah*"

Saya sudah kerja sebagai konsultan security networking selama 10 tahun,klien saya ada dari pihak perusahaan swasta,aparat keamanan indonesia,sampa pernah kerjasama dengan FBI US. Dari pengalaman saya ada tiga kemungkinan:Pertama karena TROJAN, yang Kedua karena ada yang sengaja menanam "kode" Firmware

di smartphone korban(dalam hal ini wisnu kumoro),dan yang Ketiga ada yang meng-kloning smartphone korban dari jarak jauh(level dewa).Akan saya jelaskan satu persatu.Untuk yang PERTAMA karena TROJAN,pada dasarnya teknik trojan ini meng-instal aplikasi ke smartphone korban,baik disengaja atau tidak disengaja,setelah aplikasi berhasil terinstal,maka pelaku dapat me-remote(menjalankan aksinya dari jarak jauh,seperti membuka aplikasi apapun yang ada di smartphone korban,tau password aplikasi,tau isi sms,isi email dan sbg)pokoknya bisa melakukan apapun dan tau apapun terhadap smartphone korban.Trojan ini bisa sengaja di instal lalu di hide(sehingga korban tidak tau) atau tidak sengaja ter-instal(biasanya korban dikirimi link yang menarik/manipulasi,sehingga tanpa sengaja link tersebut di klik oleh korban(biasanya tawaran diskon,promo,bonus)biasanya penawaran yg berisi link bisa lewat WA,LINE,INSTAGRAM,TWITTER dan sosmed lainnya(kalau lewat email,sudah cara kuno).Kalau yang sengaja ter-instal,bisa dilakukan oleh orang terdekat korban,yang pernah meminjam hp si korban. Untuk yang KEDUA karena ada yang sengaja menanam "kode" Firmware di smartphone korban,hal ini bisa dilakukan melalui dua cara,yaitu dari pihak teknisi si vendor smartphone atau dilakukan oleh pelaku yang telah menemukan celah atau BACKDOOR sehingga bisa menanam/menginstal kode di firmware korban. Untuk yang KETIGA ada yang meng-kloning smartphone korban dari jarak jauh,konsepnya mirip dengan yang pertama( PAKAI TROJAN)tapi bukan dgn me-instal aplikasi ke smartphone, tapi dengan memakai semacam hardware/tool,Jadi pelaku memiliki sebuah hardware/tool yg dpt mengkloning smartphone korban,dgn mengarahkan hardware tertentu ke smartphone korban(maksimal dalam radius 15 meter),cara ini di pakai oleh pihak spionase(CIA dll).Jadi kalau masalah ini di bawa ke pihak kepolisian,pasti akan dilakukan DIGITAL forensic dan Hardware Forensics. Kalau menurut saya si wisnu kumoro ini kena yg kemungkinan pertama atau kedua(TROJAN atau ada yang sengaja menanam "kode" Firmware).Kalau kemungkinan ketiga tidak mungkin(wisno kumoro bukan orang penting/pejabat) yang harus diawasi.Saran saya instal ulang OS smartphone,kalau ada update lakukan update dgn segera(karena salah satu fungsi update adalah untuk "menambal" celah/BACKDOOR sistem yang telah dieksploitasi oleh

pelaku.TOLONG TULISAN INI DISHARE KE LAINNYA/ BERI TAU WISNU KUMORO HATI2 PAKAI SMARTPHONE GRATISAN DARI VENDOR.

**2.3 Penyelesaian**

Pihak Jenius sendiri menyarankan kepada pengguna agar memblokir kartu, hal ini dilakukan agar tidak terjadi lagi penyadapan oleh *si hacker*. Setelah itu, pihak Jenius akan mengirim kartu baru kepada pengguna tersebut. Jenius juga menyarankan bagi pengguna yang baru saja mengalami kejadian seperti ini agar langsung melaporkan kejadian secepatnya serta membagikannya ceritanya ke segala platform media sosial, agar informasi dapat langsung diterima oleh pihak Jenius dan dapat segera ditangani.

# BAB III
# PENUTUP

## 3.1 Kesimpulan

Kasus transaksi siluman rekening jenius ini memang meresahkan terutama bagi mereka yang memiliki akun dan menyimpan uang mereka di rekening jenius. Pada kasus ini bisa didapat banyak sekali pelajaran bagi korban, pihak Jenius, dan para pembaca. Pada kasus ini, para pembaca diingatkan untuk lebih berhati-hati dalam menggunakan internet, terutama dalam mengakses situs finansial/perbankan. Dan bagi pihak Jenius untuk lebih memperhatikan keamanan situs mereka dan memperbaiki sistem mereka supaya hal yang sama tidak terulang kembali.

## 3.2 Kritik dan Saran

Kami sangat menyayangkan sistem keamanan Jenius yang sangat lemah. Sudah semestinya sebagai layanan perbankan, Jenius memiliki sistem keamanan yang kuat. Apalagi sistem OTP bisa dibobol, ini kurang wajar.

Kami sangat menyarankan pihak Jenius untuk meningkatkan sistem keamanan guna melindungi nasabah. Peningkatan sistem keamanan ini bisa dilakukan dengan mengadakan program *bug bounty*. Untuk itu diperlukan kerja keras agar sistem keamanan dapat diperkuat.

# DAFTAR PUSTAKA

Facebook. (2019, 2 September). E-Commerce Shitposting. Diakses pada tanggal 23 September 2020, dari https://web.facebook.com/ECommerceShitposting/posts/kali-ini-kita-mau-bahas-soal-wisnu-kumoro-yang-kemarin-kebobolan-akun-jeniusnyad/522434001835852/?_rdc=1&_rdr

Youtube. (2019, 30 Agustus). REKENING GUE DIBOBOL (Part 1). Diakses pada tanggal 23 September 2020, dari https://www.youtube.com/watch?v=O31xL58ciCI

Webbatik.com. (2020, 7 Juni). Transaksi Siluman dari Rekening Jenius. Diakses pada tanggal 3 September 2020, dari https://www.webbatik.com/2020/06/transaksi-siluman-dari-rekening-jenius.html