Evaluasi dan Analisis Security Awareness dalam Password Behavior pada Mahasiswa

Dicky Sopandi[1], Parman Sukarno[2], Rahmat Yasirandi [3]

[1,2,3] Universitas Telkom, Bandung
[1]dickysop@students.telkomuniversity.ac.id, [2]parmansukarno@telkomuniversity.ac.id, [3]batanganhitam@telkomuniversity.ac.id

Abstrak

Seiring berkembangnya teknologi, keamanan menjadi hal yang penting, dan kata sandi merupakan metode otentikasi keamanan yang masih menjadi tren hingga saat ini. Metode otentikasi keamanan apa pun tidak lemah. Masalah sebenarnya kembali ke pengguna itu sendiri, kesadaran dan pemahaman tentang keamanan adalah dasar untuk membangun keamanan. Mahasiswa merupakan salah satu contoh orang yang membutuhkan kesadaran akan keamanan informasi, dimana internet sering digunakan dalam kehidupan sehari-hari. Beberapa faktor mempengaruhi otentikasi kata sandi dan memori dan kesadaran keamanan yang juga dipengaruhi oleh latar belakang pendidikan. Oleh karena itu sampel dan populasi penelitian ini dilakukan pada siswa Generasi Z. Penelitian ini bertujuan untuk mengukur faktor latar belakang pendidikan terhadap security awareness pada siswa Generasi Z. Metode pengumpulan data menggunakan metode kuantitatif. Metode analisis yang digunakan adalah kuantitatif dan deskriptif menggunakan Usability Testing, yaitu menggunakan aplikasi penilaian Kaspersky Password Checker untuk mengetahui seberapa kuat password.

Kata kunci : kata sandi, keamanan, kesadaran, tingkah laku

Abstract

As technology develops, security is critical, and the password is a security authentication method that is still a trend today. Any security authentication method is not weak. The real problem is back to the user himself, awareness and understanding of security is the basis for building security. Students are one example of people who need information security awareness, where the internet is often used in their daily lives. Several factors affect password authentication and memory and security awareness which is also influenced by educational background. Therefore, the sample and population of this study were conducted on Generation Z students. This study aims to measure the educational background factor on security awareness in Generation Z students. The data collection method uses quantitative methods. The analytical method used is quantitative and descriptive using Usability Testing, which uses the Kaspersky Password Checker assessment application to find out how strong the password.

Keywords: password, security, awareness, behavior

1. Pendahuluan

Latar Belakang

Baru-baru ini muncul kasus peretasan terhadap mahasiswa UNDIP, dilaporkan bahwa 125 ribu data mahasiswa telah dicuri dengan informasi pribadi yang lengkap [1]. Oleh karena itu kesadaran dan pemahaman tentang keamanan adalah dasar untuk membangun keamanan yang baik dalam suatu organisasi. Bukti survei yang dipublikasikan membuktikan hal itu, pelatihan dan latar belakang pendidikan diakui memiliki hubungan yang signifikan dengan tingkat keamanan yang dapat dicapai, dan diutamakan dalam berbagai standar keamanan, banyak organisasi tidak mampu memanfaatkannya [2]. Pada saat ini masih banyak yang menggunakan otentikasi konvensional untuk keamanan akun, Sistem proses otentikasi konvensional hanya membutuhkan nama pengguna dan kata sandi untuk otentikasi. Metode ini, bagaimanapun, sangat nyaman untuk keamanan dari segala bentuk serangan serta otentikasi tanpa ijin dengan hanya menggunakan *password* dan *username* [3].

Mahasiswa memerlukan kesadaran keamanan informasi, terutama internet yang sering digunakan sehari-hari [4]. Mahasiswa sebagai generasi Z memiliki hubungan erat dengan IT dan media sosial yang umumnya menggunakan proses otentikasi konvensional, oleh karena itu pada penelitian ini mengambil sampel pada mahasiswa Telkom University.

Oleh karena itu, pada penelitian ini digunakan tiga latar belakang mahasiswa yaitu jenis kelamin, tingkat semester, dan jenis pendidikan. Diketahui tingkat perilaku keamanan wanita jauh lebih rendah daripada laki-laki. Kesadaran akan keamanan pada wanita juga lebih rendah dibandingkan laki-laki bahkan terkadang wanita tidak sadar bahwa keamanannya diserang dikarenakan tingkat perilaku keamanan yang rendah tadi [2]. Ditemukan juga bahwa mahasiswa tingkat 1 maupun tingkat 4 bahkan yang sudah lulus tidak terlalu memahami ancaman

cyber [3]. Jenjang pendidikan suatu mahasiswa tidak mempengaruhi kesadaran akan keamanan cyber namun pada penelitian ini akan diteliti lebih lanjut kesadaran pada mahasiswa IT dan non-IT.

Kata sandi adalah karakter yang disusun sebagai kunci hak atas data ataupun informasi [5]. Keamanan dengan kata sandi teks tetap paling umum digunakan untuk metode autentikasi akun. Sejak kata sandi teks yang rumit sulit di ingat, pengguna cenderung memilih kata sandi yang gampang dan mudah di ingat, akibatnya kata sandi lebih mudah ditebak, selain itu sering kali menggunakan kata sandi yang sama di berbagai akun agar mengurangi jumlah kata sandi yang harus di ingat berdasarkan akun yang dimiliki. Beberapa sistem mungkin sudah mengharuskan untuk mematuhi kebijakan agar menggunakan kata sandi yang rumit seperti mengharuskan ada beberapa huruf besar atau kecil, simbol, dan angka di dalam kata sandinya [6]. Tetapi masalah sebenarnya adalah pengguna itu sendiri, pengguna menggunakan pola huruf besar atau kecil dan angka atau simbol lainnya hanya di awal dan di akhir kata sandi, perilaku tersebut memudahkan upaya peretas akun untuk membaca pola kata sandi pengguna, perkembangan pola kata sandi baru sangat penting karena dapat mengurangi upaya peretas akun untuk menebak pola kata sandi [6].

Topik dan Batasannya

Berdasarkan uraian latar belakang yang telah dikemukakan diatas, maka perumusan masalah pada penelitian ini dapat disimpulkan sebagai berikut: "Apakah ada hubungan latar belakang mahasiswa terhadap *security awareness*?".

Tujuan

Berdasarkan perumusan masalah yang ditemukan, penelitian ini bertujuan untuk: "Melakukan kajian terhadap hubungan latar belakang mahasiswa dengan tingkat *security awareness*".

2. Studi Terkait

2.1 Password as Factor Authentication

Kata sandi (*password*) adalah metode otentikasi terbanyak digunakan dalam berbagai sistem keamanan. Password banyak digunakan karena mudah diimplementasi [7]. National Institute of Standards and Technology (NIST) mengemukakan bahwa standar kata sandi sebenarnya cukup sederhana: Kata sandi yang diberikan oleh pengguna setidaknya harus terdiri dari delapan karakter alfanumerik; kata sandi yang dibuat secara acak oleh sistem harus terdiri dari setidaknya enam karakter dan seluruhnya dapat berupa angka [8]. Tetapi baru-baru ini NIST telah memperbarui standarnya dan persyaratan baru yang paling signifikan: Sistem harus memeriksa kata sandi prospektif terhadap "Daftar yang berisi kata sandi yang umum digunakan, mudah ditebak, atau disusupi", lalu NIST secara eksplisit merekomendasikan persyaratan kata sandi kompleksitas tinggi.

Dalam dunia keamanan ada beberapa faktor-faktor yang mempengaruhi otentikasi yaitu [9] :

- *Something you know* – Ini adalah bentuk paling dasar dari otentikasi yang akrab dengan Sebagian pengguna, sesuatu yang diketahui pengguna misalnya: kata sandi atau kode PIN [9].
- *Something you have* – Bentuk otentikasi ini diwakili oleh barang yang dimiliki pengguna misalnya smartphone atau kartu identitas [9].
- *Something you are* – Otentikasi ini direpresentasikan sebagai tanda identitas dari fisik pengguna misalnya: sidik jari atau iris mata [9].
- *Someplace you are* – Bentuk otentikasi ini sesuai dengan lokasi pengguna untuk memverifikasi misalnya lokasi pengguna atau alamat IP [9].

Beberapa jurnal atau paper yang telah membuktikan bahwa kata sandi adalah faktor otentikasi di antaranya yang ditulis oleh Nilesh A. Lal, S. Prasad, & Mohammed Farik. Dalam judul A Review of Authentication Method, dan dipublikasikan pada tahun 2016. Dalam penelitiannya mereka melakukan tinjauan dalam metode otentikasi dimana kata sandi adalah salah satunya, dalam penelitiannya kata sandi merupakan metode otentikasi yang mengharuskan mengingat apa yang diketahuinya dan tidak diketahui orang lain, dengan ini kata sandi termasuk faktor keamanan yang rentan apabila pengguna lupa ataupun membocorkan kata sandinya kepada orang lain [10].

Jurnal atau paper kedua yang ditulis oleh Pamela R. Mc,C. Bell, Linda C. M., & Ronald F. DeMara. yang berjudul Evaluation of the Human Impact of Password Authentication Practices on Information Security dipublikasikan pada tahun 2004, dalam penelitiannya mereka mengevaluasi dampak kata sandi sebagai faktor otentikasi keamanan informasi [11].

2.2 Security Awareness

Kesadaran keamanan sangatlah penting dalam hidup manusia dikarenakan banyaknya cara yang bisa dimanfaatkan untuk memperoleh keuntungan maupun merusak informasi seseorang. Pengetahuan akan kesadaran keamanan seharusnya diajarkan dari jenjang sekolah serta implementasinya [12].

Program pelatihan dan kesadaran keamanan dapat dibagi dalam tiga bagian yang berbeda [13]:

- Pendidikan: Subjek harus memahami bahwa keamanan informasi sangat penting bagi organisasi. Setiap orang harus bertanggung jawab atas keamanan yang mempengaruhi lingkungan organisasi. Kesadaran keamanan bisa dipelajari melalui kursus atau juga pendidikan keamanan informasi dasar di sekolah atau perguruan tinggi [13].
- Pelatihan: Subjek harus mengetahui cara agar bisa merasa aman. Subjek harus mengetahui cara menggunakan fitur keamanan suatu aplikasi dan begitupun sebaliknya dimana aplikasi menyediakan pembelajaran cara menggunakan fitur keamanan [13]. *Something you are* – Otentikasi ini direpresentasikan sebagai tanda identitas dari fisik pengguna misalnya: sidik jari atau iris mata [9].
- Kesadaran: Gerakan menyerukan kesadaran keamanan juga perlu dilakukan. Program insentif akan mendorong subjek untuk berpartisipasi dengan fasi "menjadi sadar" lalu "menyadari" hingga "sadar" secara naluri atau terbiasa [13].

2.3 Characteristics of Research Sampling & Population

Populasi adalah data pusat suatu penelitian yang dipilih dengan kriteria tertentu. Biasanya suatu populasi yang menggunakan data suatu manusia maka populasinya juga akan seukuran dengan jumlah manusia tersebut [14]. Sampel adalah suatu bagian dari keseluruhan serta karakteristik yang dimiliki oleh sebuah Populasi [15]. Desain pengambilan sampel dari penelitian ini adalah nonprobability sampling karena besaran populasi pada penelitian ini tidak diketahui [16].

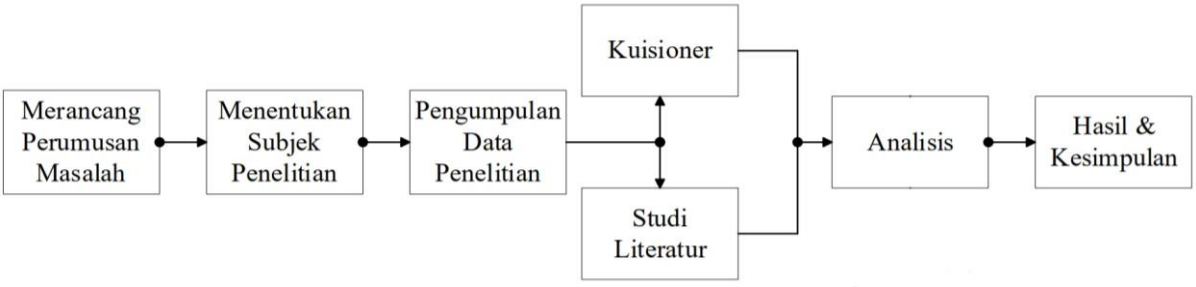
Dalam proses mengumpulkan data, terdapat juga beberapa kendala seperti: keterbatasan dana, tenaga dan waktu sehingga hanya akan digunakan beberapa bagian data populasi tersebut untuk mewakili populasi yang disebut dengan sample [15]. Oleh karena itu sampel yang didapatkan dari populasi haruslah data representatif (mewakili) yang paling akurat.

Penelitian ini menggunakan tiga perbandingan populasi yaitu latar belakang pendidikan mahasiswa, jenis kelamin dan tingkat semester. Mahasiswa merupakan generasi Z dimana sejak lahir mereka tidak lepas dari yang namanya teknologi, oleh karena itu mayoritas mahasiswa sering menggunakan internet untuk kebutuhannya. Walaupun kebutuhan mereka bermacam-macam tetapi sebagian besar mengakses media sosial, yang dimana media sosial memiliki koneksi luas tanpa batas dengan orang-orang di dunia maya. Media sosial menggunakan metode Single Factor Authentication dimana keamanannya hanyalah *username* dan *password* saja, hal ini membuat keamanan mudah ditembus. Dalam kasus ini apakah mahasiswa menyadari hal itu, untuk itu penelitian ini mengevaluasi dan menganalisis tingkat kesadaran keamanan akun mereka.

3. Sistem yang Dibangun

3.1 Flow Diagram Penelitian

Untuk membantu proses pengerjaan penelitian ini, berikut adalah alur penelitian yang dilakukan:



Gambar 1 Flow Diagram Penelitian

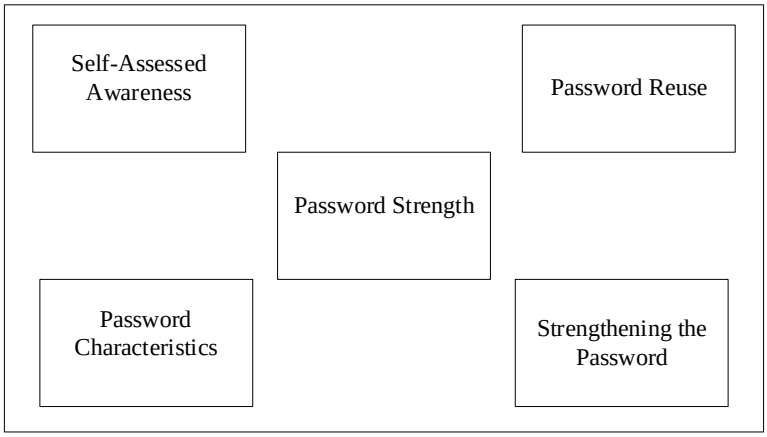
Berikut adalah uraian flow diagram penelitian yang digunakan :

1. Merancang Perumusan Masalah merupakan bagian Bab 1 yang membantu menentukan tujuan untuk penelitian yang akan dilakukan.
2. Menentukan Subjek Penelitian merupakan bagian Bab 2 yang membahas subjek sampel penelitian.

3. Pengumpulan Data Penelitian merupakan bagian Bab 3 yang membahas metode pengumpulan data, dalam penelitian ini ada dua jenis pengumpulan data yaitu:
   a) Primer: Kuisioner
   b) Sekunder: Studi Literatur
4. Metode Analisis merupakan bagian Bab 3 yang membahas metode teknik analisis data, penelitian ini menggunakan metode analisis kuantitatif.
5. Hasil Dan Kesimpulan merupakan bagian Bab 5 yang membahas hasil dari penelitian atau mendapatkan kesimpulan dan rekomendasi yang dihasilkan dalam penelitian ini.

3.2 Model Hipotesis

Hipotesis adalah dugaan sementara terhadap suatu permasalah penelitian yang menyatakan/menggambarkan hubungan dari dua variabel atau lebih sehingga harus dibuktikan dengan penyeledikan ilmiah [17]. Hipotesis yang digunakan pada penelitian ini adalah sebagai berikut:



Gambar 2 Model Hipotesis

Dari gambar diatas hipotesis dapat diuraikan sebagai berikut:

a. Self-Assessed Awareness
Untuk mendapatkan informasi terkait bagaimana kesadaran pengguna melihat sendiri keamanan kata sandi mereka, saya meminta pengguna untuk menilai sendiri keamanan kata sandi mereka.

b. Password Characteristics
Karakter *password* yang digunakan oleh pengguna biasanya menggunakan alphabetical dan numeric atau simbol lainnya, data ini sangat dibutuhkan dikarenakan untuk menemukan pola kata sandi yang kuat atau lemah dapat dibedakan berdasarkan karakter atau simbol yang dipakai, tata letak penempatan karakter ataupun jumlah karakter yang digunakan pengguna.

c. Password Strength
Selanjutnya akan membahas hasil pengukuran kekuatan kata sandi yang telah dilakukan oleh mahasiswa menggunakan Kasperski Password Checker. Bagian ini bertujuan untuk mengetahui seberapa kuat kata sandi bertahan lama, dengan adanya data ini dapat membantu penilaian kata sandi sehingga mendapatkan persentase perbandingan dengan subjek penelitian lainnya.

d. Password Reuse
Menggunakan kembali kata sandi yang digunakan atau menggunakan kata sandi yang sama di beberapa akun yang berbeda dapat menambah peluang peretas untuk meretas semua akun yang dimiliki, maka dari itu selanjutnya akan menghitung jumlah rata-rata mahasiswa yang memakai kata sandi yang sama di beberapa akun.

e. Strengthening the Password
Untuk mengetahui *password* yang kuat, peserta melakukan pengetesan untuk mencoba memperbaiki kata sandi mereka, seperti dengan menambahkan beberapa karakter dengan penempatan yang berbeda sehingga *password* lebih baik dari sebelumnya.

3.3 Metode Penelitian

Metode kuantitatif meneliti data dari sample yang dianalisis secara kuantitatif/statistik untuk menguji hipotesis yang telah ditetapkan [15]. Sebelumnya penelitian yang hampir serupa pernah dilakukan. Dengan menggunakan beberapa metode yang sama dalam pengumpulan data kuesioner dapat membantu proses pengerjaan penelitian ini.

3.3.1 Metode Pengumpulan Data

Untuk membantu pengerjaan penelitian ini, maka diperoleh metode pengumpulan data sebagai berikut :

3.3.1.1 Teknik Pengumpulan Data Primer

Data primer adalah data yang dikumpulkan langsung oleh peneliti itu sendiri dari objek atau lokasi penelitian menggunakan kuesioner. Skala likert digunakan untuk mengukur kesadaran responden terhadap kata sandi yang digunakan. Skala ini menilai sikap atau tingkah laku responden terhadap keamanan akun yang dimilikinya.

Dengan menggunakan kuisioner sebagai metode pengumpulan data, didapat contoh penilaian sebagai berikut:

	Sangat buruk	Buruk	Sedang	Baik	Sangat baik
Kekuatan kata sandi	○	○	○	○	○
Panjang kata sandi	○	○	○	○	○
Kombinasi kata sandi	○	○	○	○	○

Gambar 3 Contoh Penilaian Kuesioner

Hal yang perlu diperhatikan oleh peneliti dalam menggunakan metode kuesioner adalah sebagai berikut [18]:

- Bahwa subyek (responden) adalah orang yang paling tahu tentang dirinya sendiri [18].
- Bahwa apa yang dinyatakan oleh subyek kepada peneliti adalah benar dan dapat dipercaya [18].
- Bahwa interpretasi subyek terhadap pertanyaan-pertanyaan yang diajukan oleh peneliti terhadap subyek adalah sama dengan yang dimaksud oleh peneliti [18].

3.3.1.2 Teknik Pengumpulan Data Primer

Teknik pengumpulan data sekunder merupakan teknik pengumpulan data dengan mengumpulkan dokumen, peta, foto, atau data baik softcopy maupun hardcopy yang berasal dari penelitian sebelumnya. Teknik pengumpulan data yang digunakan adalah studi literatur yaitu mempelari studi terkait permasalah penelitian, buku, hingga artikel online maupun offline.

3.3.1.3 Teknik Pengolahan Data

Peneliti menggunakan Microsoft Excel sebagai alat untuk mengolah data responden. Microsoft Excel digunakan sebagai pengolah data dikarenakan telah dikategorikan sebagai software yang baik dan dapat digunakan sebagai pengolah data tugas akhir [5]. Dari data responden tersebut akan dibagi menjadi tiga kategori yaitu: jenis pendidikan, jenis kelamin dan tingkat semester yang nantinya ketiga kategori tersebut akan dijadikan perbandingan. Hasil data diolah menjadi grafik persentase agar memudahkan proses analisis data.

3.3.2 Analisis Data

Dari hasil pengolahan data akan diperoleh perbandingan dari tiga kategori data responden yang nantinya akan dianalisis menggunakan metode berikut.

3.3.2.1 Kuantitatif & Deskriptif

Metode penelitian kuantitatif dan deskriptif telah menjadi prosedur yang sangat umum ketika melakukan penelitian, Istilah penelitian kuantitatif dan penelitian deskriptif terkadang digunakan secara bergantian. Namun, perbedaan di antara keduanya yaitu satu hal yang mendasar adalah karakteristik kedua jenis penelitian ini melibatkan keaslian data. Tujuan penelitian deskriptif adalah mendeskripsikan suatu karakteristik dan fenomenanya [19].

Pengukuran *usability testing* dilakukan dengan menggunakan aplikasi Kaspersky Password Checker yang bertujuan untuk mengetahui klasifikasi tingkat keamanan kata sandi pengguna, pengukuran menggunakan user testing dimana pengukuran berfokus pada pengujian secara langsung. Setelah melakukan testing pengguna akan di berikan form kuesioner yang di dalamnya berupa beberapa pertanyaan terkait keamanan kata sandi mereka, pertanyaan akan berfokus pada :

- Panjang kata sandi.
- Penggunaan spesial karakter pada kata sandi.
- Penggunaan nomor pada kata sandi.
- Penggunaan huruf besar atau kecil pada kata sandi.
- Kekuatan kata sandi.
- Penggunaan ulang kata sandi.

Setelah mendapatkan data dari pertanyaan kuesioner tersebut, lalu data akan diolah dijadikan tabel diagram agar mempermudah perincian hasil penelitian.

4. Evaluasi

4.1 Hasil Pengujian

Hasil pengumpulan data dari mahasiswa yang ikut serta dalam penelitian ini berjumlah 72 mahasiswa, dalam pengujian penelitian ini untuk perbandingan data mahasiswa yang ikut serta akan dibagi menjadi tiga parameter kategori yaitu jenis kelamin, jenis pendidikan dan tingkat semester. Yang bertujuan untuk menilai seberapa besar pengaruhnya dalam ketiga kategori tersebut, dan data yang diperoleh adalah sebagai berikut:

Tabel 1 Tabel Responden Mahasiswa

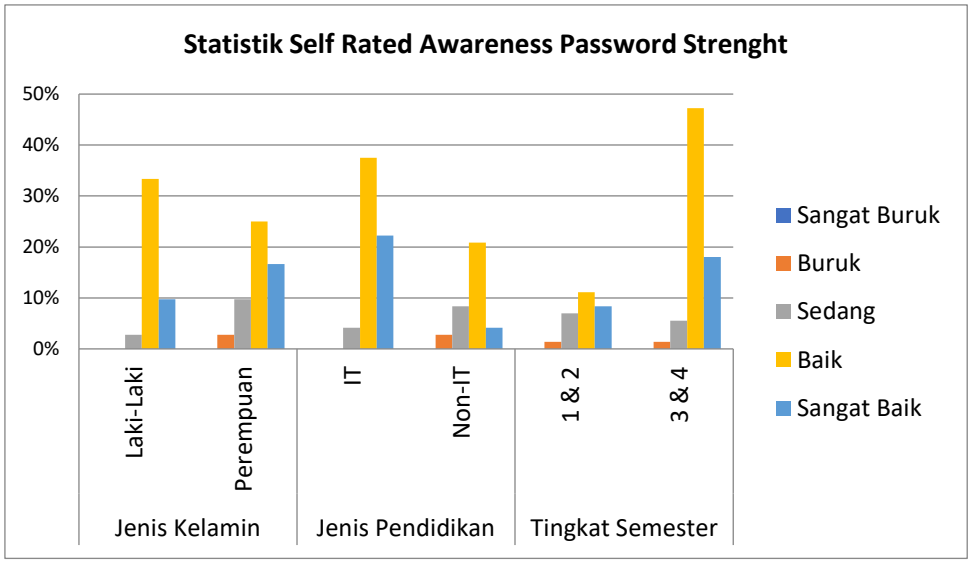
Jenis Kelamin		Jenis Pendidikan		Tingkat Semester	
Laki-laki	Perempuan	IT	Non-IT	1 & 2	3 & 4
33	39	46	26	20	52

4.1.1 *Self-Assessed Awareness*

Untuk melihat seberapa kesadaran responden dalam hal keamanan *password* yang mereka miliki, responden dalam penelitian ini dimintai untuk menilai sendiri seberapa kuat *password* mereka dengan memilih kategori dari Sangat Buruk sampai dengan Sangat Baik. Dalam uji *Self-Assessed Awareness* ini ada dua penilaian yaitu:

a. *Password Strength*

Dalam penilaian *Password Strength* ini bertujuan untuk mengetahui seberapa sadar mereka terhadap kekuatan kata sandi mereka sendiri, dengan hasil perbandingan sebagai berikut:

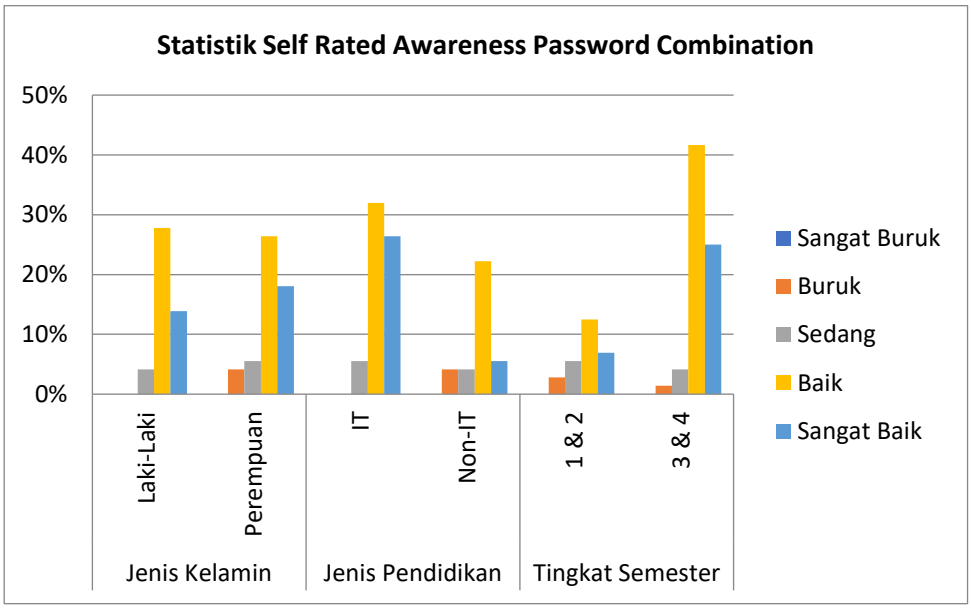


Gambar 4 Statistik *Self-Assessed Awareness* : *Password Strength*

Statistik data diatas menunjukkan bahwa perbandingan dari tiga kategori sangat berbeda dimulai dari jenis kelamin, laki-laki cenderung percaya diri akan kekuatan kata sandinya sedangkan perempuan memiliki jawaban yang beragam tetapi juga kebanyakan memilih jawaban baik/sangat baik, lalu dari jenis pendidikan dan tingkat semester, jenis pendidikan IT dan tingkat semester atas yaitu 3 dan 4 memiliki kepercayaan yang sangat baik terhadap kekuatan kata sandi mereka, sedangkan jenis pendidikan Non-IT dan tingkat semester bawah tingkat 1 dan tingkat 2 rata-rata jawabannya adalah buruk sampai baik di sini menunjukkan bahwa mereka kurang percaya diri terhadap kata sandi miliknya.

b. *Character Combination*

Character Combination yaitu sebuah deretan karakter huruf, angka dan simbol lainnya dalam sebuah kata sandi. Dalam penilaian *Character Combination* ini bertujuan untuk menilai seberapa sadar responden terhadap kombinasi karakter kata sandi yang mereka miliki, dengan hasil perbandingan sebagai berikut:

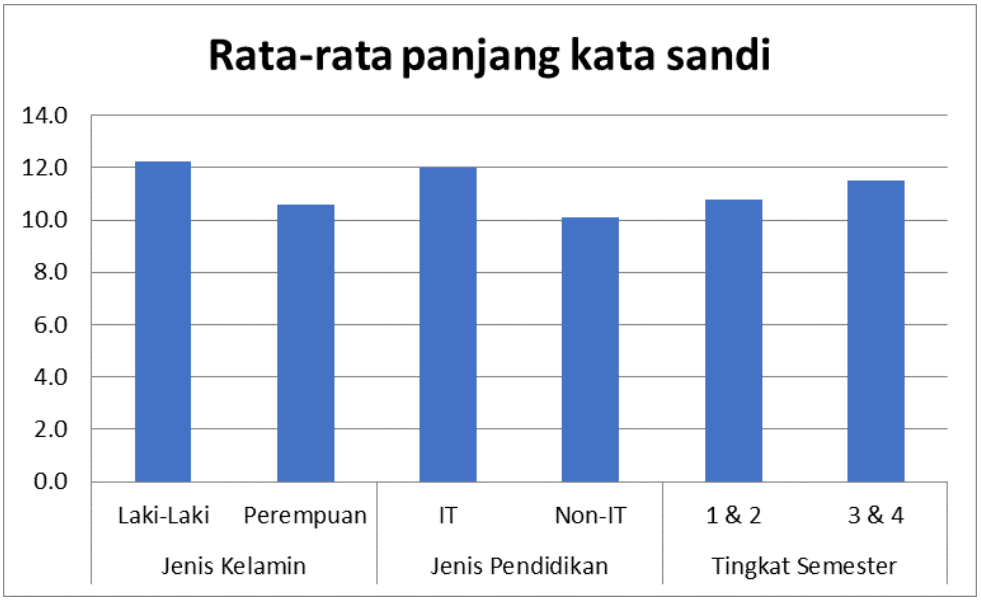


Gambar 5 Statistik *Self-Assessed Awareness* : *Character Combination*

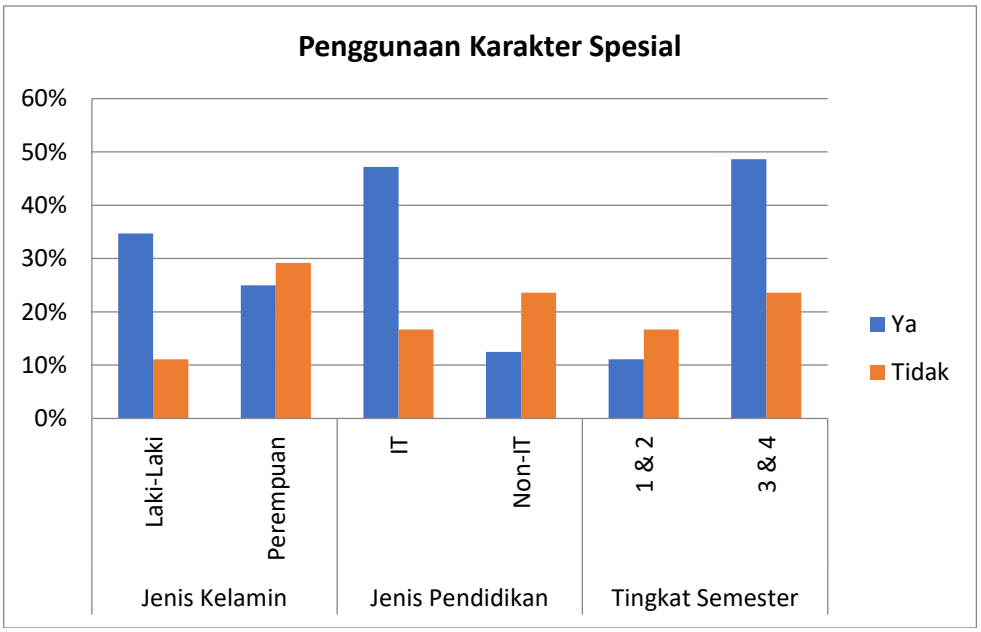
Untuk statistik data *Character Combination* dari jenis kelamin laki-laki dan jenis pendidikan IT tidak terlalu beda jauh, keduanya sama-sama mempunyai rata-rata sekitar 30% untuk penilaian baik, tetapi IT mempunyai persentase nilai sangat baik yang hampir seimbang. Lalu jenis kelamin perempuan dengan jenis pendidikan Non-IT hampir mirip bedanya hanya pada penilaian sangat baik pada jenis kelamin perempuan lebih tinggi sedangkan jenis pendidikan Non-IT sangat rendah jika dibandingkan dengan jenis kelamin perempuan. Dan dari kategori tingkat semester, tingkat 1 dan tingkat 2 memiliki tingkat kepercayaan yang sedang sehingga jawaban mereka menjadi beragam, sedangkan tingkat 3 dan tingkat 4 memiliki tingkat kepercayaan yang tinggi dengan persentase nilai baik dan sangat baik paling tinggi.

4.1.2 *Password Characteristics*

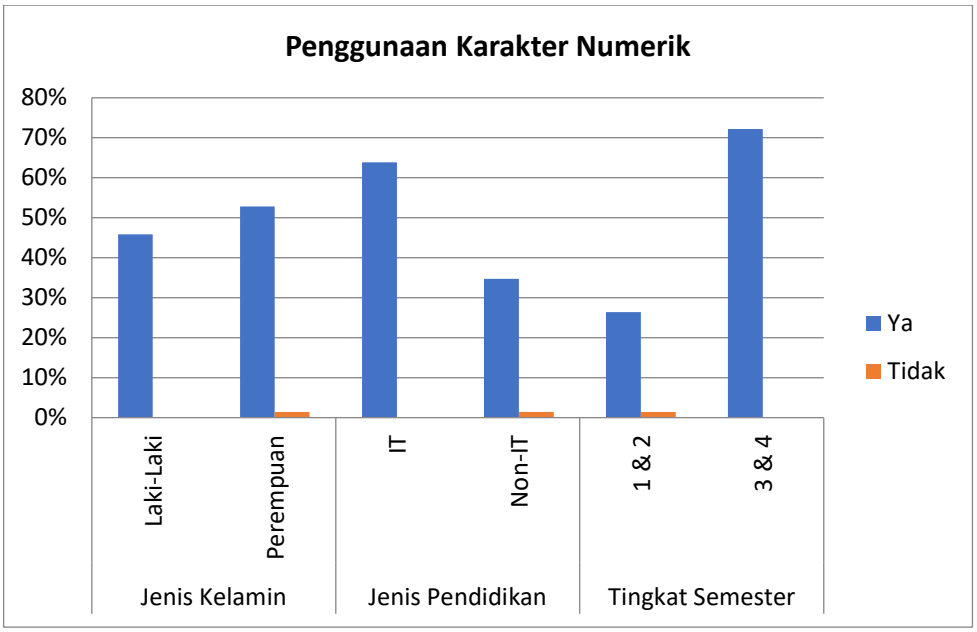
Dalam penelitian ini dibutuhkan keterangan kata sandi lebih lanjut seperti panjang kata sandi, penggunaan karakter spesial, penggunaan karakter numerik, penggunaan elemen nama, dan penggunaan huruf besar/kecil, oleh karena itu responden diberikan pertanyaan mengenai hal tersebut dan diperoleh data sebagai berikut:



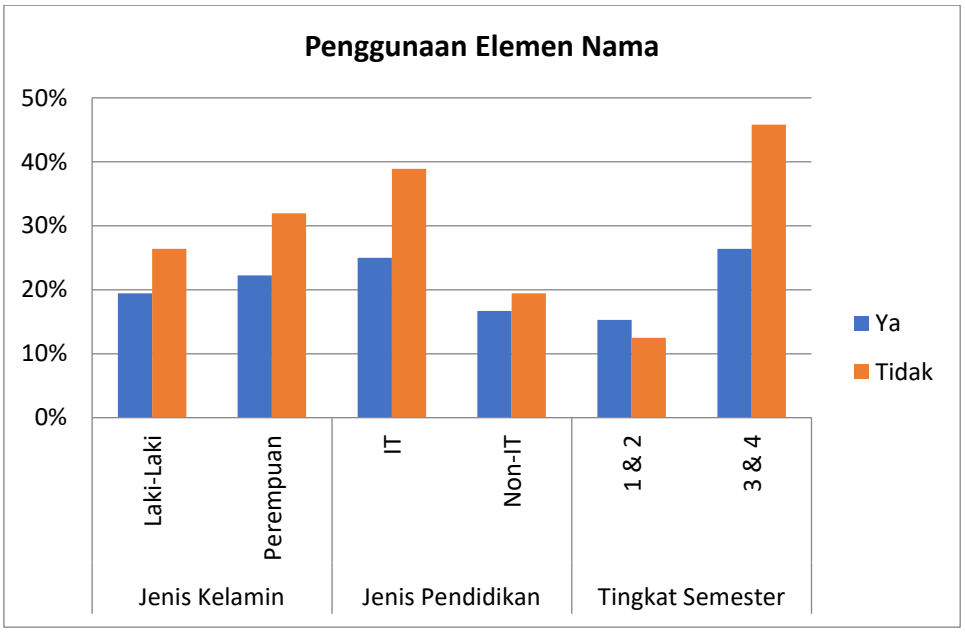
Gambar 6 Rata-rata panjang kata sandi



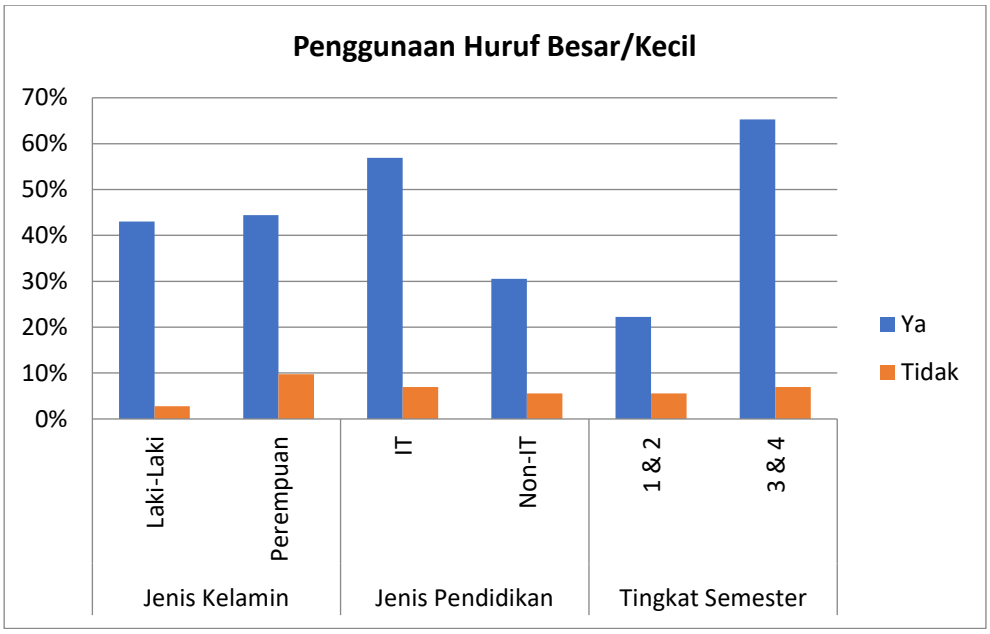
Gambar 7 Penggunaan Karakter Spesial



Gambar 8 Statistik Penggunaan Karakter Numerik



Gambar 9 Statistik Penggunaan Elemen Nama

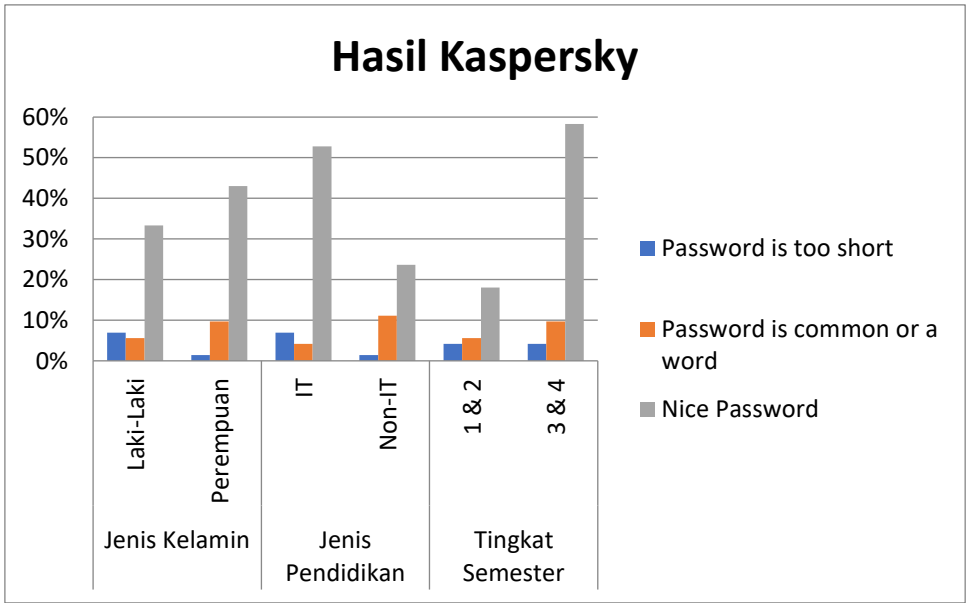


Gambar 10 Penggunaan Huruf Besar/Kecil

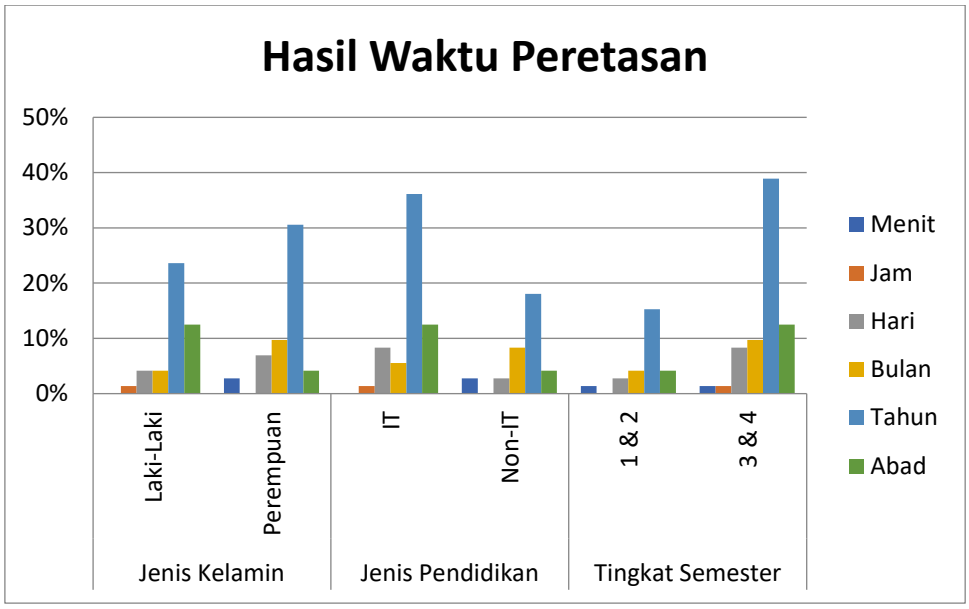
Dari segi panjang kata sandi dari keseluruhan sudah mencapai angka yang cukup, lalu disusul oleh penggunaan huruf besar kecil dan penggunaan karakter numerik sudah sangat baik. Tetapi dalam penggunaan elemen nama dan penggunaan karakter spesial di sini masih lebih banyak yang tidak memakai dimana hasil responden banyak jawaban yang masih kurang diharapkan.

4.1.3 *Password Strength*

Pada pengujian *password strength* kata sandi yang dipilih oleh responden yang telah dicek menggunakan kaspersky password checker. Maka akan didapat hasil apakah kata sandi tersebut Bagus, Terlalu pendek atau Mengandung kata-kata yang ada di kamus besar. Selain itu kaspersky password checker akan menunjukkan hasil berapa lama kata sandi responden bertahan lama jika diretas, berikut adalah hasil data yang diperoleh:



Gambar 11 Statistik Hasil Kaspersky

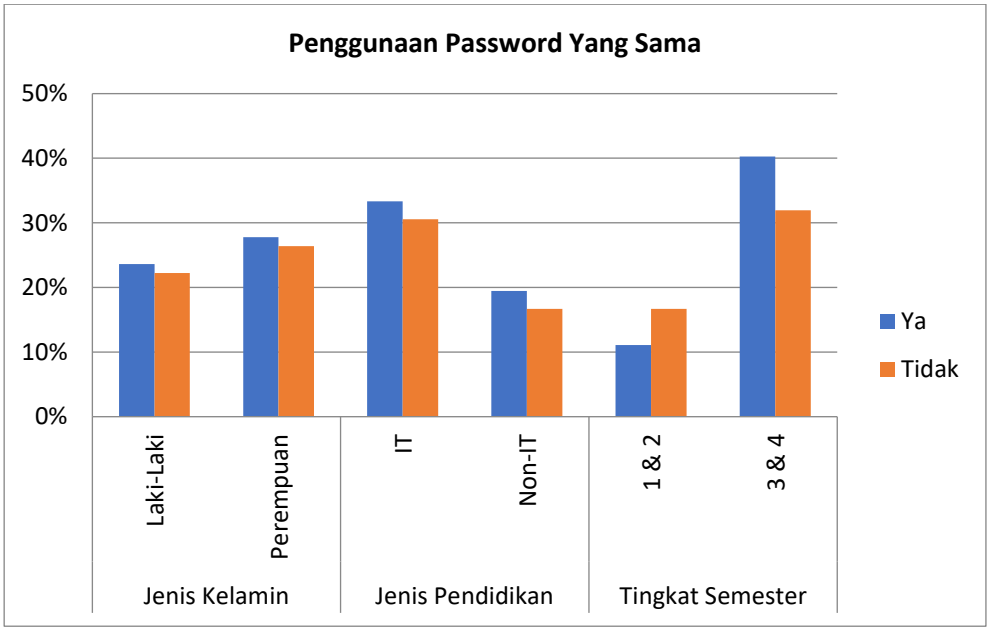


Gambar 12 Statistik Hasil Waktu Jika Diretas

Dari dua diagram diatas menunjukkan bahwa hasil dari pengecekan kata sandi kaspersky password checker yaitu rata-ratanya dari semua kategori, hasil yang paling tinggi adalah *nice password* lalu untuk hasil waktu yang di tunjukan yang paling tinggi adalah tahunan.

4.1.4 *Password Reuse*

Menggunakan kembali kata sandi yang sama di banyak akun sekaligus dapat melipat gandakan kerugian akibat pembobolan kata sandi, oleh karena itu dalam penelitian ini responden ditanyai apakah mereka menggunakan kata sandi yang dipakai lebih dari dua akun atau lebih, berikut adalah data yang telah didapat:



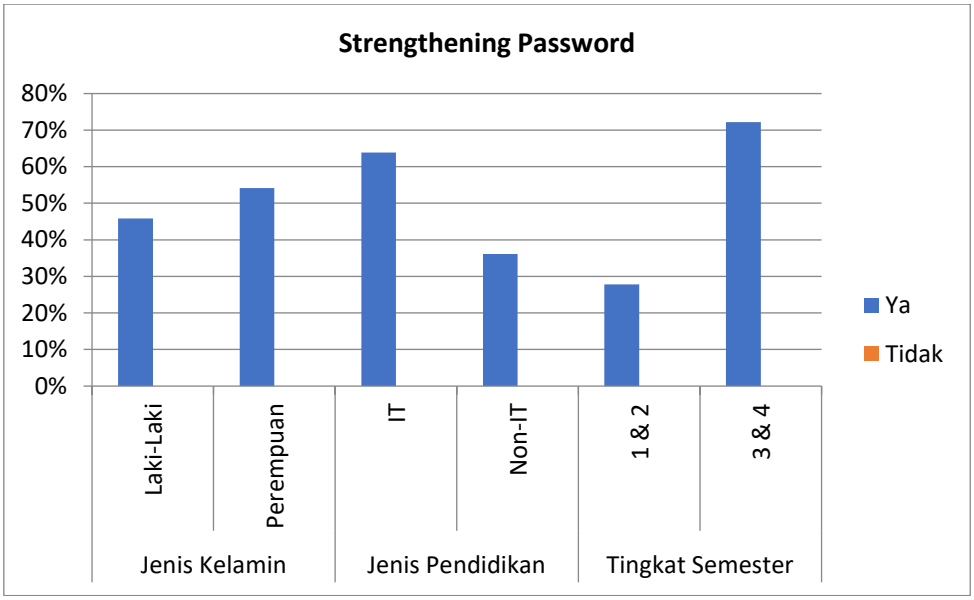
Gambar 13 Statistik Penggunaan *Password* Yang Sama

Dari semua jenis kategori, responden kebanyakan menggunakan ulang kata sandinya di beberapa akun lain, hampir sama dengan yang menjawab tidak kecuali tingkat semester 1 dan 2 mereka lebih banyak memilih tidak.

4.1.5 *Strengthening the Password*

Strengthening the password yaitu uji penguatan kata sandi dengan cara melakukan pengecekan ulang menggunakan kaspersky password checker tetapi dengan menggunakan kata sandi yang tetap lalu menambahkan

simbol atau karakter spesial seperti "?" pada ujung kata sandi. Responden ditanyai ada perbedaan mengenai kemajuan yang ada pada hasil pengecekan atau tidak ada kemajuan sama sekali.



Gambar 14 Statistik Hasil Penambahan Karakter Spesial

Pada diagram statistik diatas dari kategori jenis kelamin hingga kategori tingkat semester semuanya menjawab "Ya", yang berarti dalam penambahan simbol atau karakter spesial sangat membantu penguatan kata sandi.

4.2 Analisis Hasil Pengujian

Untuk menganalisis hasil pengaruh kondisi-kondisi yang berbeda, pada penelitian ini menggunakan tiga parameter kategori responden yang diambil, dan untuk perbandingan diambil data persentase yang paling tinggi dari setiap model hipotesis yang ada.

4.2.1 Jenis Kelamin

Dari keseluruhan data responden yang di kumpulkan, jumlah responden laki-laki adalah 46% sedangkan perempuan adalah 54%. Dari dua jenis kelamin tersebut didapatkan hasil perbandingan sebagai berikut:

Tabel 2 Statistik Penggunaan *Password* Yang Sama

Perbandingan Berdasarkan Jenis Kelamin			
Model Hipotesis		**Laki-laki**	**Perempuan**
Self-Assessed Awareness	Kekuatan Kata Sandi	33% Baik	25% Baik
	Kombinasi Kata Sandi	25% Baik	26% Baik
Password Characteristics	Rata-rata Panjang Kata Sandi	12,2	10,6
	Penggunaan Karakter Spesial	35% Ya	29% Tidak
	Penggunaan Karakter Numerik	46% Ya	53% Ya
	Penggunaan Elemen Nama	26% Tidak	32% Tidak
	Penggunaan Huruf Besar/Kecil	43% Ya	44% Ya
Password Strength	Hasil Kaspersky	33% Nice	43% Nice
	Hasil Waktu Diretas	24% Tahun	31% Tahun
Password Reuse	Penggunaan Ulang Kata Sandi	24% Ya	28% Ya
Strengthening the Password	Penambahan Karakter Spesial	46% Ya	54% Ya

Berdasarkan dari tabel diatas dalam hal kesadaran tentang keamanan kata sandi keduanya baik laki-laki maupun perempuan menunjukkan hasil dalam kekuatan dan kombinasi kata sandi paling tinggi adalah baik, sedangkan jika kita bandingkan dengan hasil yang ditunjukkan oleh kaspersky kedua hasilnya sama yaitu *Nice* Password dan dengan hasil waktu jika diretas adalah rata-rata tahunan, ini cukup bagus tetapi dalam penggunaan

ulang kata sandi keduanya menunjukkan bahwa rata-rata mereka menjawab "Ya" yang berarti ini sangat berisiko jika salah satu akun diretas.

Pada penelitian [20] dijelaskan persepsi perempuan tentang informasi keamanan, bahwa tingkat pengguna perempuan sangat tinggi dalam pengaruh yang ditimbulkan oleh ancaman keamanan informasi bagi mereka dibandingkan laki-laki. Tetapi pengguna perempuan merasa percaya diri tentang keamanan informasi yang dimilikinya walaupun mereka mengakui bahwa kurangnya keterampilan dalam bidang IT. Sedangkan dijelaskan dalam penelitian [21] laki-laki lebih cenderung memiliki pengalaman yang lebih baik di bidang IT dan hasil penelitian menunjukkan bahwa laki-laki memiliki perilaku keamanan informasi yang lebih baik dan dilindungi lebih daripada perempuan.

4.2.2 Pendidikan

Lalu dari parameter jenis pendidikan terdapat dua jenis yaitu IT dan Non-IT, yang berjumlah berdasarkan data responden adalah 64% dari IT dan 36% dari Non-Teknik. Dan didapat hasil perbandingan sebagai berikut:

Tabel 3 Perbandingan Berdasarkan Jenis Pendidikan

Perbandingan Berdasarkan Jenis Pendidikan			
Model Hipotesis		**IT**	**Non-IT**
Self-Assessed Awareness	Kekuatan Kata Sandi	38% Baik	21% Baik
	Kombinasi Kata Sandi	32% Baik	22% Baik
Password Characteristics	Rata-rata Panjang Kata Sandi	12,0	10,1
	Penggunaan Karakter Spesial	47% Ya	24% Tidak
	Penggunaan Karakter Numerik	64% Ya	35% Ya
	Penggunaan Elemen Nama	39% Tidak	19% Tidak
	Penggunaan Huruf Besar/Kecil	57% Ya	31% Ya
Password Strength	Hasil Kaspersky	53% Nice	24% Nice
	Hasil Waktu Diretas	36% Tahun	16% Tahun
Password Reuse	Penggunaan Ulang Kata Sandi	33% Ya	19% Ya
Strengthening the Password	Penambahan Karakter Spesial	64% Ya	36% Ya

Pada perbandingan antara jenis pendidikan yaitu IT dan Non-IT, kesadaran keduanya menunjukkan kekuatan dan kombinasi kata sandinya baik, dan untuk *password characteristics* semuanya bagus kecuali untuk Non-IT dalam penggunaan karakter spesial rata-rata paling tinggi menjawab "Tidak" di sini sangat disayangkan karena tidak memakai karakter spesial, mungkin penyebabnya juga di jurusan Non-IT karena pengaruh lingkungan kurangnya interaksi dengan hal-hal yang membahas tentang keamanan informasi.

Hasil dari analisis ini bahwa mahasiswa jurusan bidang IT lebih memahami keamanan informasi karena pengalaman yang mereka miliki berbeda jauh dengan jurusan Non-IT, seperti yang di jelaskan pada penelitian [22] Bahwa pengguna komputer pada mahasiswa lebih memahami tentang keamanan informasi lebih daripada pengguna *smarthpones* dikarenakan pengalaman pengguna yang berbeda. lalu pada penelitian [23] mereka meneliti kemampuan para pekerja yang bekerja pada bidang Non-IT terhadap *cybersecurity*, hasil pada penelitiannya menunjukkan bahwa memang pekerja dari bidang Non-IT berbeda jauh kemampuannya dari pekerja IT, tetapi dalam penelitian itu menegaskan bahwa pekerja dari bidang Non-IT pun wajib mengembangkan kemampuannya untuk menangani *cybersecurity*.

4.2.3 Tingkat Semester

Dan dari parameter tingkat semester dibagi menjadi dua bagian yaitu tingkat bawah (semester 1 dan 2) dan tingkat atas (semester 3 dan 4), didapatkan jumlah persentase responden dari tingkat bawah sebesar 28% dan dari tingkat atas sebesar 72%. Dan hasil perbandingan sebagai berikut:

Tabel 4 Perbandingan Berdasarkan Jenis Pendidikan

Perbandingan Berdasarkan Tingkat Semester			
Model Hipotesis		**1 & 2**	**3 & 4**
Self-Assessed Awareness	Kekuatan Kata Sandi	11% Baik	47% Baik
	Kombinasi Kata Sandi	13% Baik	42% Baik

Password Characteristics	Rata-rata Panjang Kata Sandi	10,8	11,5
	Penggunaan Karakter Spesial	17% Tidak	49% Ya
	Penggunaan Karakter Numerik	26% Ya	72% Ya
	Penggunaan Elemen Nama	15% Ya	46% Tidak
	Penggunaan Huruf Besar/Kecil	22% Ya	65% Ya
Password Strength	Hasil Kaspersky	18% Nice	58% Nice
	Hasil Waktu Diretas	15% Tahun	39% Tahun
Password Reuse	Penggunaan Ulang Kata Sandi	17% Tidak	40% Ya
Strengthening the Password	Penambahan Karakter Spesial	28% Ya	72% Ya

Lalu pada perbandingan berdasarkan tingkat semester dibagi menjadi dua kelompok yaitu tingkat semester bawah (1 dan 2) dan tingkat semester atas (3 dan 4), pada keduanya menunjukkan tingkat kesadaran yang cukup baik tetapi pada *password characteristics* untuk tingkat bawah cukup rentan karena rata-rata dari mereka tidak menggunakan karakter spesial dan lebih buruknya lagi mereka menggunakan elemen nama seperti nama sendiri atau keluarga atau bisa saja menggunakan nama tempat asal atau tempat kelahiran, di sini memudahkan peretas untuk menemukan atau menebak kata sandi berdasarkan identitas target, tetapi dari tingkat bawah banyak yang tidak menggunakan ulang kata sandinya sedangkan dari tingkat atas banyak yang menggunakan ulang ini lebih berisiko karena jika satu akun berhasil diretas maka akun lainnya kemungkinan mudah diretas.

Pada paper [24] membahas tentang pentingnya kesadaran keamanan informasi pada mahasiswa, terkait kasus *cyber security* mahasiswa menjadi target utama dalam upaya *Phising*, dikarenakan jumlah waktu penggunaan di internet tinggi ini menjadikannya lebih berisiko. Oleh karena itu dalam penelitiannya membahas jauh lebih dalam pentingnya edukasi atau pelatihan dalam mengenai *security awareness* pada mahasiswa.

5. Kesimpulan

5.1 Rekomendasi

5.1.1 Edukasi

Berdasarkan hasil penelitian ini, saya mengusulkan rekomendasi yang pertama yaitu mengedukasi mahasiswa lebih dini, yang bertujuan untuk mengajarkan bahwa betapa pentingnya kata sandi yang kuat agar kesadaran mahasiswa pada penggunaan ulang kata sandi di beberapa akun terhindar dan mengajarkan membuat kata sandi yang beragam dan kompleks tetapi mudah di ingat, ini bertujuan untuk memudahkan penggunaan kata sandi rumit yang berbeda di setiap akunnya, seperti peletakan karakter yang harus diperhatikan selain menempatkan huruf besar/kecil hanya diawali kata sandi saja tetapi bisa juga di bagian-bagian lain seperti di tengah atau secara acak begitu pun dengan penggunaan karakter spesial dan angka [3].

5.1.2 Kebijakan

Membuat kebijakan kata sandi yang umum seperti panjang minimum karakter, penggunaan nomor, huruf besar/kecil, dan penggunaan spesial karakter sesuai ketentuan National Institute of Standards and Technology (NIST).

5.1.3 Sistem

Akan lebih baik jika sistem otomatis memeriksa atau mendeteksi kata sandi pengguna sebelum membuat akun, seperti pemeriksaan kesamaan kata sandi apakah mengandung *username* atau nama pengguna di dalamnya, itu akan menghindari kebiasaan pengguna dalam membuat kata sandi yang mengandung nama.

5.2 Kesimpulan

Dalam penelitian ini dari tiga kategori perbandingan yaitu jenis kelamin, jenis pendidikan dan tingkat semester. Mulai dari jenis kelamin laki-laki semua indikasi model hipotesis yang digunakan menunjukkan hasil yang sangat bagus dari misalnya karakteristik kata sandi yang digunakan sudah mengikuti standar yang ada sedangkan perempuan karakteristik kata sandinya masih kurang misalnya kurangnya dalam penggunaan karakter spesial, walaupun hanya menambahkan satu karakter spesial tetapi hasil yang di tunjukan oleh kaspersky jauh lebih baik daripada sebelumnya yang tidak menggunakan karakter spesial, dalam hal ini laki-laki jauh lebih mengerti tentang kombinasi karakter kata sandi yang baik daripada perempuan. Lalu dari jenis pendidikan mulai dari jurusan IT/Teknik dan Non-IT hasilnya sama persis dengan kategori jenis kelamin yaitu dari jurusan IT/Teknik menunjukkan hasil yang sama seperti kategori jenis kelamin laki-laki sedangkan jurusan Non-IT menunjukkan hasil yang sama seperti jenis kelamin perempuan, seperti yang dibahas sebelumnya karakter spesial berperan penting dalam pengaruh kekuatan kata sandi, yang berarti dari kebanyakan mahasiswa di jurusan IT/Teknik lebih paham tentang membuat kata sandi yang kompleks dibandingkan dengan jurusan Non-

IT. Dan yang terakhir dari kategori tingkat semester yaitu tingkat bawah (tingkat 1 dan 2) dan tingkat atas (tingkat 3 dan 4), untuk tingkat bawah hasil yang ditunjukkan masih sangat kurang jika dilihat dari indikasi model hipotesis karakteristik kata sandi, dimulai dari penggunaan karakter spesial yang kurang dan yang lebih buruknya lagi yaitu rata-rata dari mereka menggunakan elemen nama pada kata sandinya yang memungkinkan lebih mudah menebaknya dibandingkan dengan kata sandi yang tidak mengandung elemen nama, sedangkan tingkat semester atas telah mencapai standar yang ditetapkan dalam hal karakteristik kata sandi, yang artinya di sini tingkat bawah masih jauh pengetahuan mereka tentang pentingnya kekuatan kata sandi maka dari itu sebaiknya mereka diajari tentang kesadaran kekuatan kata sandi sejak dini.

Tetapi dari tiga kategori tersebut memiliki kesamaan kecuali dari kategori tingkat semester yaitu semester tingkat bawah (tingkat 1 dan 2), yaitu memiliki kesamaan tentang penggunaan ulang kata sandi mereka pada akun lainnya hal ini sangat krusial walaupun hasil yang di tunjukan oleh kaspersky bagus tetapi jika salah satu kata sandi diretas maka kemungkinan akun lainnya pun bisa saja ikut teretas, maka dari itu sekali lagi kurangnya pendidikan tentang hal ini membuat mereka tak acuh dalam penggunaan ulang kata sandi.

REFERENSI

[1] Liputan6, "Lebih dari 125 Ribu Data Mahasiswa UNDIP Bocor," 2021. https://www.liputan6.com/tekno/read/4449390/lebih-dari-125-ribu-data-mahasiswa-undip-bocor.

[2] S. Furnell and N. Clarke, "Organizational security culture: Embedding security awareness, education, and training," *Proc. 4th World Conf. Inf. Secur. Educ.*, vol. 11, no. Dti, pp. 67–74, 2005.

[3] R. Yasirandi, P. Sukarno, and F. A. Laguliga, "Context Awareness Adoption for Authentication Process in Log In System (Case Study: PT. XYZ)," *Int. J. Comput. Digit. Syst.*, vol. 10, pp. 1–14, 2020.

[4] Z. Hidayat, A. Saefuddin, and S. Sumartono, "Motivasi, Kebiasaan, dan Keamanan Penggunaan Internet," *J. ILMU Komun.*, vol. 13, no. 2, p. 129, Jan. 2017, doi: 10.24002/jik.v13i2.675.

[5] Hermawan and A. Saputra, "Studi Tingkat Password Policy Mahasiswa Program Studi Pendidikan Teknik Informatika, Pendidikan Bahasa Inggris, dan Pendidikan Matematika Universitas Negeri Yogyakarta," *Teknol. Inf.*, 2012.

[6] M. Awad, Z. Al-Qudah, S. Idwan, and A. H. Jallad, "Evaluating Password Behavior at a Small University," *J. Comput. Sci.*, vol. 15, no. 1, 2019, doi: 10.3844/jcssp.2019.1.9.

[7] W. Sudiarto Raharjo, I. D. E.K. Ratri, and H. Susilo, "Implementasi Two Factor Authentication Dan Protokol Zero Knowledge Proof Pada Sistem Login," *J. Tek. Inform. dan Sist. Inf.*, vol. 3, no. 1, 2017, doi: 10.28932/jutisi.v3i1.579.

[8] P. Grassi *et al.*, "Digital Identity Guidelines: Authentication and Lifecycle Management," *Spec. Publ. (NIST SP) - 800-63B*, 2017, doi: 10.6028/nist.sp.800-63b.

[9] W. Kennedy and A. Olmsted, *Three Factor Authentication*. 2017.

[10] M. Farik, N. Lal, and S. Prasad, "A Review Of Authentication Methods," *Int. J. Sci. Technol. Res.*, vol. 5, pp. 246–249, Nov. 2016.

[11] D. S. Carstens, P. R. McCauley-Bell, L. C. Malone, and R. F. DeMara, "Evaluation of the human impact of password authentication practices on information security," *Informing Sci.*, vol. 7, pp. 67–85, 2004, doi: 10.28945/503.

[12] M. Amin, "Information Security Awareness Level Measurement Using Multiple Criteria Decision Analysis (Mcda)," *J. Penelit. dan Pengemb. Komun. dan Inform.*, vol. 5, no. 1, p. 122371, 2014.

[13] T. Schlienger and S. Teufel, "Information security culture – from analysis to change," *South African Comput. J.*, vol. 31, pp. 46–52, 2003.

[14] Margono, "Metodologi Penelitian Pendidikan. Jakarta: Rineka Cipta," 2010.

[15] Sugiyono, *Metode Penelitian Kuantitatif, Kualitatif dan R&D. Bandung: PT Alfabet*. 2016.

[16] Indrawati, "Metode Penelitian Manajemen dan Bisnis Konvergensi Teknologi Komunikasi dan Informasi," *Bandung PT Refika Aditama*, p. 285, 2015.

[17] Y. A. Muri, "Metodologi Penelitian (Dasar-dasar Penyelidikan Ilmiah). Padang: Unp Press," 2005.

[18] Sugiyono, "Metode Penelitian Bisnis. Bandung : Alfabeta," 2012.

[19] H. Nassaji, "Qualitative and descriptive research: Data type versus data analysis," *Lang. Teach. Res.*, vol. 19, no. 2, pp. 129–132, 2015, doi: 10.1177/1362168815572747.

[20] T. McGill and N. Thompson, "Gender differences in information security perceptions and behaviour," *ACIS 2018 - 29th Australas. Conf. Inf. Syst.*, 2018, doi: 10.5130/acis2018.co.

[21] F. Alotaibi and A. Alshehri, "Gender Differences in Information Security Management," *J. Comput. Commun.*, vol. 08, no. 03, pp. 53–60, 2020, doi: 10.4236/jcc.2020.83006.

[22] N. Taha and L. Dahabiyeh, "College students information security awareness: a comparison between smartphones and computers," *Educ. Inf. Technol.*, vol. 26, no. 2, pp. 1721–1736, 2021, doi: 10.1007/s10639-020-10330-0.

[23] M. Carlton, Y. Levy, and M. Ramim, "Mitigating cyber attacks through the measurement of non-IT professionals' cybersecurity skills," *Inf. Comput. Secur.*, vol. 27, no. 1, pp. 101–121, 2019, doi: 10.1108/ICS-11-2016-0088.

[24] T. Hunt, "Cyber Security Awareness in Higher Education," *Cent. Washingt. Univ.*, pp. 1–14, 2016.

[25] F. B. Fatokun, S. Hamid, A. Norman, and J. O. Fatokun, "The Impact of Age, Gender, and Educational level on the Cybersecurity Behaviors of Tertiary Institution Students: An Empirical investigation on Malaysian Universities," *J. Phys. Conf. Ser.*, vol. 1339, no. 1, 2019, doi: 10.1088/1742-6596/1339/1/012098.

Lampiran

Kategori	Sangat Buruk	Buruk	Sedang	Baik	Sangat Baik
Kekuatan	Responden merasa kata sandinya sangat lemah.	Responden merasa kata sandinya lemah.	Responden merasa kata sandinya sudah cukup.	Responden merasa kata sandinya kuat.	Responden merasa kata sandinya sangat kuat.
Kombinasi	Kata sandi tidak memiliki satupun kombinasi karakter spesial, huruf besar/kecil, dan angka.	Kata sandi memiliki salah satu dari kombinasi karakter spesial, huruf besar/kecil, atau angka.	Kata sandi memiliki dua kombinasi dari salah satu karakter spesial, huruf besar/kecil, atau angka.	Kata sandi memiliki semua kombinasi karakter spesial, huruf besar/kecil, dan angka.	Kata sandi memiliki semua kombinasi karakter spesial, huruf besar/kecil, angka, dan penempatan karakter yang acak.