# KEJAHATAN SIBER

"adalah aktivitas kriminal yang melibatkan komputer, perangkat lunak, atau jaringan internet. Walaupun sebagian besar kejahatan siber dilakukan untuk menghasilkan keuntungan bagi pelaku, beberapa kasus kejahatan siber dilakukan untuk merusak atau menonaktifkan komputer atau perangkat lunak secara langsung."

4 Hal yang dapat Anda lakukan untuk menjaga diri Anda aman dari kejahatan siber

**1. Aktifkan autentikasi multifaktor**

Dengan menerapkan autentikasi multifactor, kemungkinan terjadinya serangan siber akan semakin berkurang

**2. Perbaharui perangkat lunak**

Memperbarui perangkat lunak secara berkala dapat mengurangi secara signifikan risiko terhadap serangan kejahatan siber.

**3. Berpikir dua kali sebelum mengklik**

Berhati-hati sebelum mengklik tautan apa pun karena sebagian besar kasus kejahatan siber berasal dari phishing email.

**4. Gunakan kata sandi yang kuat**

Jangan gunakan kata sandi yang sama berulang kali di semua aplikasi dan akun.

Edukasi tentang bahaya ancaman siber juga perlu terus digaungkan melalui media apapun agar masyarakat lebih teredukasi mengenai digital

# Jenis Kejahatan Siber

### Serangan DDos

Membuat situs dan jaringan terganggu dengan cara membanjiri situs dengan berbagai macam *traffic online*

### Pencurian Identitas

Memperoleh akses ke informasi pribadi pengguna

### Rekayasa Sosial

Membuat kontak langsung dengan korban melalui telfon atau email dengan berpura-pura menjadi pihak lain

### Pengelabuan *email*

Peretas mengirim lampiran email atau URL berbahaya ke pengguna

### Penipuan Daring

Penipuan berupa iklan atau email spam yang berisi janji atau hadiah dan penawaran

### *Cyberstalking*

Pelaku menggunakan media sosial, situs web, dan mesin pencari untuk mengintimidasi pengguna asli

### PUPs

"Program yang Mungkin Tidak Diinginkan" bentuk kejahatan sejenis malware ini mungkin kurang mengancam daripada yang lain

### Mengeksploitasi KITs

Bug dalam kode perangkat lunak untuk mendapatkan kendali atas komputer pengguna

# Kasus Kejahatan Siber

## Contoh Serangan pada Email yang ditargetkan

Subjek: Undangan Seminar Kemanan Infomasi untuk Perusahaan Keuangan

Dari:****@***.com

Untuk: .....@abc.com

Dengan hormat,

Melalui email ini, kami memberitahukan bahwa akan diadakan seminar pembahasan laporan dan hasil diskusi yang bekerja sama dengan Universitas dan Zenginkyo pada bulan Mei 2020.

Sesi pengarahan, yang didasarkan pada hasil kuesioner, akan sangat membantu para pemangku kepentingan lembaga keuangan dalam mempertimbangkan masa depan dan arah keamanan informasi di lembaga keuangan. Silakan lihat juga laporan terlampir.

Kami menantikan partisipasi aktif Anda.Untuk detailnya, lihat undangan terlampir.Anda dapat mendaftar untuk seminar dari alamat di bawah ini.Karena kapasitas ruang seminar terbatas, kami menyarankan Anda untuk segera mendaftarmungkin.
Formulir pendaftaran ⇒ https://www.abc.com

Lampiran:

Subjek dan teks dirancang untuk menarik target.

Disarankan untuk mengkonfirmasi alamat sumber dengan hati-hati. Dalam beberapa tahun terakhir, **pengirim terkadang berpura-pura menjadi perusahaan nyata dengan *email* perusahaan**

Pengirim berkamuflase untuk menyamarkan bagian URL situs web resmi sehingga tidak dapat dibedakan dari aslinya secara sekilas.

**Tujuan tautan juga dapat ditulis dengan kata-kata yang meyakinkan sehingga membuat Anda ingin membuka tautan yang tertera.**

Penggunaan file Word, Excel dan CSV atau aplikasi Microsoft Office lainnya sedang marak. *File extensions* juga dapat diubah.

**Melampirkan file Ms. Word sebagai lampiran sudah menjadi kasus yang umum untuk serangan seperti ini.**

## Kejahatan Siber dalam lintas platform *Instant Messaging*

Mereka akan meminta Anda untuk merahasiakan percakapan anda dengan pelaku

Penipu akan mencoba menghubungi Anda secara tiba-tiba. Mereka berpura-pura menjadi seseorang yang Anda kenal.

Mereka akan menciptakan situasi yang tampak seperti urgensi dan akan membuat Anda berada di bawah tekanan untuk merespons dengan cepat.

Penipu akan mencoba mendapatkan detail pribadi atau keuangan Anda. Kasus terbaru adalah mengirimkan file *apk untuk mengelabui target agar mengklik. Setelah mengklik, detail pribadi dan keuangan target akan bocor dan diretas oleh penipu.

## BCA Mobile Apps – Virus pada Aplikasi Pop Up

- Modus dugaan penipuan viral terbaru di aplikasi BCA Mobile berupa pop-up notifikasi dengan tampilan seolah-olah meminta pengguna menghapus virus saat akan membuka BCA Mobile.
- Virus ini dapat menyebabkan perangkat diakses oleh aplikasi jarak jauh tanpa otorisasi. Modus penipuan di aplikasi BCA Mobile menyerupai modus Android Package Kit (APK, format file .apk).
- Peretas menargetkan data kredensial (nama pengguna dan kata sandi) dan data keuangan dengan misi mengendalikan akun perbankan target.
- Jika pop-up tersebut muncul dan diklik, maka file .apk akan otomatis terpasang dan ponsel pengguna disusupi malware. Terakhir, data pengguna dapat dimiliki oleh peretas.