

# OUCH!

## Dalam Edisi Ini...

- Sekilas
- Lima Langkah Sederhana
- Tetap Aman Saat Anak Bertamu

## Mengajarkan Pentingnya Keamanan

### Sekilas

Sebagian dari kita merasa nyaman dengan teknologi, termasuk menggunakannya dengan tepat dan benar. Namun, tidak jarang adarekan dan keluarga beranggapan lain. Mereka sering merasa gagap/bingung, terintimidasi dan bahkan takut teknologi. Ini menyebabkan mereka mudah menjadi sasaran penyerang siber. Pengamanan dunia siber tidaklah demikian menakutkan, bahkan boleh dibbilang sederhana bila dimengerti dasar pemikirannya.

Mereka ini hanya perlu bimbingan dari Anda untuk bisa mengerti hal-hal mendasar tersebut.

### Editor Tamu

Randy Marchany (Twitter: [@randymarchany](https://twitter.com/randymarchany)) adalah CISO di Virginia Tech dan instruktur bersertifikat di SANS Institute.

### Lima Langkah Sederhana

Berikut ini adalah lima langkah sederhana untuk membantu orang lain dalam mengatasi rasa takut dan menggunakan teknologi sebaik mungkin. Untuk mendapatkan penjelasan lebih rinci setiap langkah, simak daftar pustaka dibagian akhir buletin ini.

1. **Rekayasa Sosial:** Teknik ini sering digunakan oleh penyerang siber untuk memperdaya atau menggiring seseorang agar melakukan tindakan yang semestinya tidak dilakukan, seperti berbagi sandi, memicu penyebaran virus ke dalam komputer atau memberikan informasi sensitif. Sejak ribuan tahun lalu, segala tipu daya dan pelaku kejahatan seperti itu sudah lama ada. Hanya saja sekarang konsep tersebut diterapkan di dunia internet. Kita bisa menjelaskan kepada orang lain perihal ciri-ciri serangan rekayasa sosial, seperti saat seseorang menciptakan suasana serba terburu-buru, bila sesuatu terasa mengada-ada atau saat seorang penyerang siber berpura-pura menjadi teman baik namun cara berkirim pesan tidak seperti biasanya. Beri beberapa contoh serangan rekayasa sosial seperti surel pengelabuan, atau telepon dari layanan teknis Microsoft. Juga pastikan setiap anggota keluarga tidak pernah berbagi sandi kepada siapapun dan juga memberikan akses komputer jarak jauh.
2. **Sandi:** Perlindungan peralatan dan akun daring membutuhkan sandi yang kuat. Jelaskan cara menciptakan sandi yang kuat. Disarankan menggunakan frasa-sandi lantaran mudah digunakan sekaligus diingat. Frasa-sandi pada dasarnya adalah sandi yang dirangkai dari beberapa kata. Selain itu, bantu memasang pengelola sandi. Setiap

## Mengajarkan Pentingnya Keamanan

peralatan dan akun harus menggunakan sandi berbeda. Bisa pengelola sandi dirasa terlalu rumit, ajarkan mencatat dan menyimpan dengan aman semua sandi tersebut. Selanjutnya, untuk akun penting, bantu aktifkan verifikasi dua tahap (disebut juga sebagai otentifikasi dua faktor). Verifikasi dua tahap merupakan salah satu cara paling efektif dalam menjaga keamanan sebuah akun.

3. **Penyempurnaan:** Memastikan penggunaan sistem teranyar dan terkini termasuk langkah penting dalam menjaga keamanan peralatan. Aturan ini tidak hanya berlaku untuk komputer dan gawai/alkom saja, namun juga semua peralatan yang tersambung ke internet seperti piranti game, pengukur suhu dan bahkan lampu dan speaker. Aktifkan fasilitas pembaruan otomatis bila memungkinkan.
4. **Anti-Virus:** Setiap orang bisa melakukan kekeliruan, mengklik atau memasang sesuatu yang semestinya tidak dilakukan karena berpotensi menginfeksi sistem yang ada. Anti-virus dirancang bisa memberikan perlindungan terhadap kekeliruan tersebut. Memang anti-virus tidak mungkin menapis semua program berbahaya/malware, namun setidaknya mengenal dan menghentikan serangan yang bersifat umum. Pastikan anti-virus terpasang di setiap komputer di rumah serta dalam kondisi terkini dan aktif. Perlu diingat, banyak solusi anti-virus belakangan ini mencakup juga teknologi keamanan lainnya seperti firewall dan proteksi peramban/browser.
5. **Pencadangan:** Dalam situasi terburuk, cadangan/backup adalah satu-satunya cara pemulihan berbagai hal seperti keliru menghapus berkas atau menjadi korban ransomware. Pastikan keluarga dan teman menggunakan sistem pencadangan otomatis. Terkadang, solusi termudah adalah menggunakan solusi berbasis Cloud dengan metode pencadangan berkala atau pada saat terjadi perubahan isi berkas. Solusi itu memudahkan proses pencadangan dan juga unduh ulang.



*Bantu orang lain memanfaatkan teknologi secara aman dengan mengenalkan lima langkah sederhana pengamanan.*

## Tetap Aman Saat Anak Bertamu

Bila Anda merasa nyaman menggunakan teknologi, pasti juga akan memastikan keamanan anak-anak Anda. Saat berkunjung ke tempat keluarga yang tidak nyaman atau gagap dalam penggunaan teknologi seperti kakek-nenek, mereka mungkin tidak mengerti cara terbaik melindungi anak-anak saat daring sesuai harapan Anda. Berikut ini adalah beberapa cara perlindungan keamanan anak-anak saat berkunjung ke keluarga lain atau famili.

## Mengajarkan Pentingnya Keamanan

- **Aturan:** Pastikan ada aturan atau batasan bagi anak-anak yang diketahui pihak keluarga. Contoh: berapa lama bisa daring, kepada siapa bisa berkirim pesan, games apa yang boleh dan tidak boleh dimainkan. Percayalah, jangan berharap anak-anak menjelaskan aturan tersebut ke sanak famili. Tidak ada salahnya menyiapkan 'lembar aturan' dan menyerbarkannya ke sanak famili yang sering dikunjungi.
- **Kendali:** Bila seorang anak lebih mengenal seluk beluk teknologi dari orang disekitarnya, bisa saja mereka memanfaatkan kondisi tersebut. Misal, anak meminta akses hak administrator di komputer kakek-nenek untuk melakukan banyak hal seperti memasang games yang seharusnya tidak boleh dimainkan. Pastikan sanak saudara paham agar tidak memberikan akses diluar yang ada sekarang

Yang tidak kalah penting, anjurkan berlangganan buletin OUCH! Agar proses belajar secara mandiri tetap berlanjut. Buletin ini diterbitkan setiap bulan, dalam lebih dari 20 bahasa. Daftarkan diri di <https://securingthehuman.sans.org/ouch>.

## Selanjutnya

Untuk berlangganan buletin bulanan OUCH! Kesadaran Keamanan, mengakses arsip buletin OUCH! dan mengetahui lebih banyak solusi kesadaran keamanan SANS, silakan kunjungi [securingthehuman.sans.org/ouch/archives](https://securingthehuman.sans.org/ouch/archives).

## Versi Bahasa Indonesia

BIPIMax memberikan Pelatihan Optimasi Proses Bisnis (LSS) dan Pengenalan Keamanan & Proteksi Informasi. Informasi lengkap: <http://www.bipimax.net>

## Daftar Pustaka

Rekayasa Sosial:	<a href="https://securingthehuman.sans.org/ouch/2017#january2017">https://securingthehuman.sans.org/ouch/2017#january2017</a>
Frasa-sandi:	<a href="https://securingthehuman.sans.org/ouch/2017#april2017">https://securingthehuman.sans.org/ouch/2017#april2017</a>
Pengelola Sando:	<a href="https://securingthehuman.sans.org/ouch/2017#september2017">https://securingthehuman.sans.org/ouch/2017#september2017</a>
Verifikasi Dua Tahap:	<a href="https://securingthehuman.sans.org/ouch/2015#september2015">https://securingthehuman.sans.org/ouch/2015#september2015</a>
Pencadangan & Unduh Ulang:	<a href="https://securingthehuman.sans.org/ouch/2017#august2017">https://securingthehuman.sans.org/ouch/2017#august2017</a>
Daring Sehat Bagi Anak:	<a href="https://securingthehuman.sans.org/ouch/2017#may2017">https://securingthehuman.sans.org/ouch/2017#may2017</a>

OUCH! diterbitkan oleh SANS "Securing The Human" dan didistribusikan sesuai lisensi [Creative Commons BY-NC-ND 4.0](https://creativecommons.org/licenses/by-nc-nd/4.0/). Anda diperkenankan menyebarkan buletin ini atau menggunakannya di dalam program pembelajaran sejauh tidak melakukan perubahan isi buletin. Untuk keperluan alih bahasa atau informasi lainnya, silakan menghubungi [ouch@securingthehuman.org](mailto:ouch@securingthehuman.org).

Dewan Redaksi: Walt Scrivens, Phil Hoffman, Cathy Click, Cheryl Conley  
Diterjemahkan oleh: T. Gunawan



[securingthehuman.sans.org/blog](https://securingthehuman.sans.org/blog)



[/securethehuman](https://securethehuman)



[@securethehuman](https://twitter.com/securethehuman)



[securingthehuman.sans.org/gplus](https://securingthehuman.sans.org/gplus)