PEMERINTAH KABUPATEN
HULU SUNGAI UTARA
DINAS KOMINFO & SANDI

BerAKHLAK
Berorientasi Pelayanan Akuntabel Kompeten
Harmonis Loyal Adaptif Kolaboratif

#bangga melayani bangsa

LAKSA Literasi Keamanan Siber dan Sandi #002

Bajalanan ke Kota Martapura
Basama dangsanak wan kaluarga
Walau hati riang wan gembira
Tatap waspada ancaman di dunia maya ...

8 Jenis Ancaman Keamanan pada Perangkat Digital

Apakah pernah akun media sosialmu diretas? Atau pernah mendengar cerita dari orang sekitarmu yang mengalami kejadian itu? Itu adalah contoh ancaman keamanan pada perangkat digital. Paling tidak terdapat 8 jenis ancaman keamanan yang perlu kita waspadai, yaitu:

1 Kebocoran Data (*data leakage*)

Banyak aplikasi-aplikasi yang tersedia di internet yang kita pasang di ponsel kita tetapi terkadang kita tidak sadar bahwa aplikasi tersebut bisa mengakses data-data yang ada di ponsel kita, seperti kontak, penyimpanan, kamera, dan sebagainya. Oleh karena itu selalu hati-hati saat memasang aplikasi di ponsel kita dan perhatikan akses yang diminta.

2 Gangguan pada Wi-fi (*Wi-fi interference*)

Kita sering terhubung ke layanan Wi-Fi umum dan gratis yang tersedia di banyak tempat dan kita sering tidak tahu apakah jaringan tersebut aman atau tidak. Oleh karena itu, jika terhubung dengan Wi-Fi umum hindari memasukkan info sensitif atau melakukan transaksi keuangan yang memerlukan data seperti kartu kredit atau transaksi perbankan.

3 Perangkat lunak yang tidak diperbarui (*out-of-date devices*)

Perangkat lunak dari setiap aplikasi di ponsel kita biasanya memberikan pembaruan (update) dalam periode waktu tertentu, yang bertujuan untuk memperbarui versi aplikasi, termasuk didalamnya pembaruan untuk celah keamanan yang diketahui pernah ada. Jika tidak diperbarui, risiko keamanan ponsel kita menjadi lebih besar karena terdapat celah tersebut.

4 Rekayasa sosial (*social engineering*)

Terkadang tidak perlu teknologi rumit untuk meretas atau mencuri data pribadi orang. Melalui rekayasa sosial, kita bisa melakukannya dengan misalnya berpura-pura sebagai orang lain untuk menggali informasi pribadi korban, memberikan tautan (link) palsu untuk mengelabui korban, dan sebagainya.

5 Serangan C*ryptojacking* (*cryptojacking attacks*)

Ini ancaman keamanan yang relatif baru. *Cryptojacking* adalah jenis serangan dimana seseorang menggunakan perangkat orang lain untuk menambang *cryptocurrency* tanpa sepengetahuan pemiliknya. Ponsel yang mengalami hal ini mungkin akan cepat habis baterainya dan bahkan dapat mengalami kerusakan karena komponen yang terlalu panas.

6 Penipuan melalui Iklan seluler (*mobile ad fraud*)

Terdapat aplikasi di ponsel yang disisipi oleh malware, sebuah program yang menyusup ke dalam ponsel kita untuk melakukan aktivitas tertentu, dalam hal ini adalah menjalankan iklan tertentu yang akan menguntungkan pembuat malware. Malware ini dapat berjalan di ponsel kita tanpa kita sadari dan memperlambat kinerja ponsel, menghabiskan baterainya, menimbulkan biaya data yang lebih tinggi, atau menyebabkan panas berlebih.

7 Pengelolaan kata sandi yang buruk (*poor password hygiene*)

Menggunakan kata sandi yang mudah ditebak, kata yang sama untuk berbagai akun dan tidak mengaktifkan 2FA, adalah contoh pengelolaan kata sandi yang buruk, sehingga perangkat dan akun media sosial kita rentan diretas.

8 Kebocoran melalui perangkat secara fisik (*physical device breaches*)

Ponsel yang tidak dijaga serta tidak dikunci, memiliki kemungkinan juga untuk dapat diakses oleh orang-orang yang tidak bertanggung jawab.

sumber : BSSN

#SandiKami
#jagaruangsiber

AGUNG GOVERNMENT CSIRT KABUPATEN HULU SUNGAI UTARA

Jalan Norman Umar, Amuntai (0527) 6061127 csirt@hsu.go.id diskominfo.hsu.go.id