LAPORAN AKTIVITAS PHISHING DOMAIN ~.ID

Indonesia Anti-Phishing Data Exchange

IDADX

Periode Q4 2023

Oktober – Desember 2023

Daftar Isi

Ruang Lingkup Laporan Phishing

Laporan tren aktivitas phishing IDADX menganalisis serangan phishing dan pencurian identitas lainnya pada nama domain .id. Laporan ini didapatkan dari hasil data APWG yang dilaporkan oleh anggotanya di http://www.apwg.org, dan melalui email kiriman ke reportphishing@antiphishing.org.
Dalam laporan ini, kami juga mengumpulkan data phishing dari Netcraft yang dikirimkan melalui email. Selain itu, IDADX juga mendapatkan laporan dari anggotanya yang dilaporkan melalui situs web http://idadx.id, dan laporan phishing dari masyarakat.

Definisi Phishing

Phishing adalah sebuah kejahatan dengan upaya mendapatkan informasi pribadi seseorang hingga kredensial akun keuangan. Pada saat ini, phishing biasanya dilakukan dengan skema *social engineering* dan *technical subterfuge*. *Social engineering* mengincar korban yang tidak waspada dengan memanipulasi mereka agar percaya bahwa mereka berurusan dengan pihak yang tepercaya dan sah, seperti mengirimkan pesan penipuan melalui alamat email. *Technical Subterfuge* menanam malware ke komputer untuk mencuri informasi kredensial dari korban, biasanya menggunakan sistem yang mencegat nama pengguna dan kata sandi atau mengarahkan pengguna ke situs web palsu. Sebagai akibat dari penipuan ini, semakin banyak konsumen yang menderita penipuan kartu kredit, pencurian identitas, dan kerugian finansial.

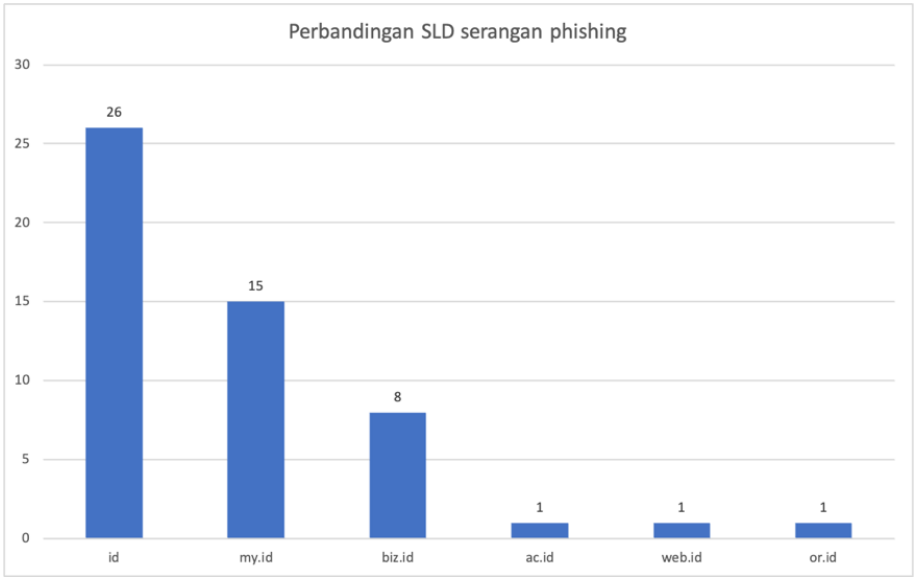
Ringkasan Laporan Phishing

- IDADX mendapatkan laporan phishing sebanyak 106.806 selama kurun waktu 5 tahun terakhir sejak tahun 2018.
- Jumlah serangan phishing pada Q4 2023 sebanyak 8.161 dimana mengalami penurunan dari kuartal sebelumnya.
- Total domain yang digunakan phishing pada Q4 2023 sebanyak 53 nama domain.
- Sektor media sosial paling sering menjadi serangan phishing dengan persentase 64,34 pada kuartal keempat.
- Jumlah merek/brand yang diserang sebanyak 63 brand.
- Serangan terhadap lembaga keuangan mengalami penurunan di tahun 2023. Namun pada kuartal keempat 2023, lembaga keuangan menempati urutan kedua dengan persentase sebanyak 20.58%.

Statistik Laporan Phishing Pada Q4 2023

Jumlah laporan phishing yang diterima oleh IDADX dalam kuartal keempat 2023 sebanyak 8.161, dimana mengalami penurunan sebanyak 1.662 laporan phishing dari kuartal ketiga 2023. Berdasarkan laporan phishing tersebut, sebanyak 8.024 laporan phishing merupakan data phishing https://s.id.

Pada Q4 2023 terdapat sebanyak 8.161 url phishing, dimana data tersebut berasal dari 53 domain yang berbeda. Beberapa SLD yang menjadi sasaran phishing yaitu id, my.id, biz.id, ac.id, dan web.id, or.id.

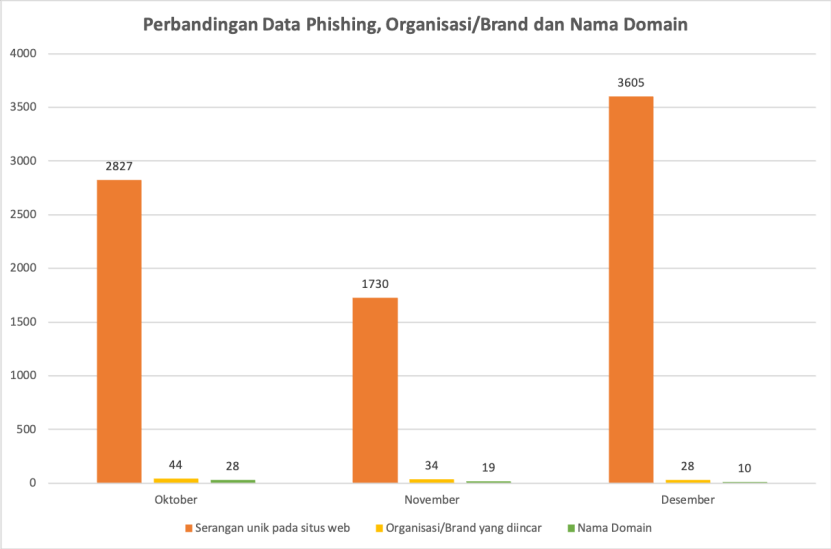


Laporan phishing selama tahun 2023 memiliki jumlah yang bervariasi dimana laporan phishing tertinggi terjadi pada bulan Februari 2023 sebanyak 15.050 dan laporan phishing terendah terjadi pada bulan November 2023 sebanyak 1.729.

Organisasi/Brand yang menjadi sasaran phishing

Grafik berikut menggabungkan statistik berdasarkan situs web phishing unik, nama merek unik, dan nama domain unik. Berikut ini penjelasan dari masing-masing data:

- **Situs web phishing**, hal ini merupakan tolok ukur utama phishing yang dikumpulkan pada dashboard IDADX.
- **Nama organisasi**, setiap URL yang dilaporkan mengandung nama organisasi/brand yang dicantumkan. Jumlah nama organisasi/brand diambil berdasarkan kelompok organisasi/brand yang unik.
- **Nama domain,** URL link mengandung nama domain yang sifatnya unik. Beberapa serangan phishing menggunakan subdomain. Biasanya, dari beberapa subdomain yang berbeda, berisi jenis phishing yang sama. Metrik ini mengukur jumlah nama domain unik sehingga tidak ada redudansi data nama domain.



Pada data tersebut dapat dilihat bahwa, pada bulan Desember merupakan jumlah laporan phishing tertinggi selama periode kuartal keempat.

Pengelompokan Serangan Phishing	Oktober	November	Desember
Total Phishing	2827	1730	3605
Organisasi/Brand yang diincar	44	34	28
Nama Domain	28	19	10

Berikut ini merupakan daftar 10 nama organisasi/brand yang menjadi target serangan phishing pada Q4 2023:

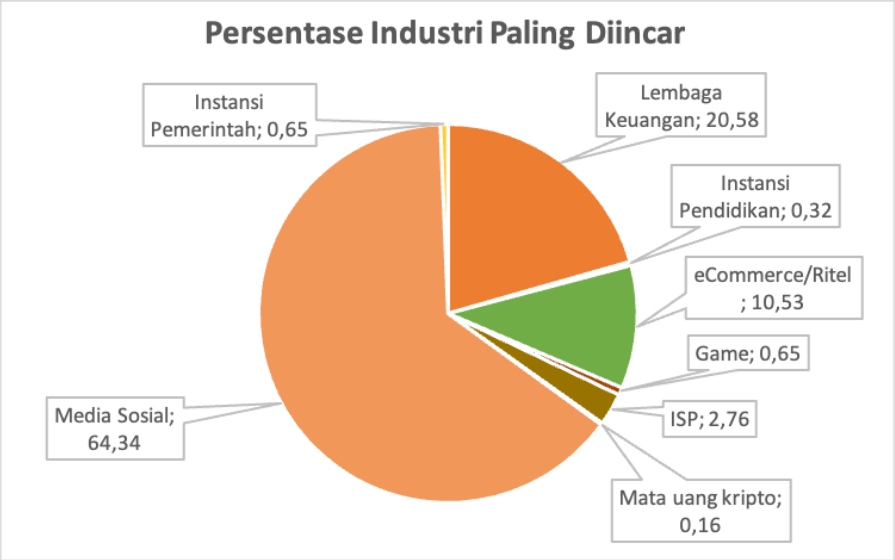
No	Organisasi/Brand
1	Facebook
2	Meta
3	Instagram
4	Whatsapp
5	At&T
6	NBT bank
7	Nexi
8	First National Bank of South Africa
9	Mercadolibre
10	Naver

Negara yang Menghosting Situs Phishing Domain .id

Indonesia menempati posisi teratas sebagai negara yang menghosting situs phishing domain .id selama Q4 tahun 2023 dan dilanjutkan pada posisi kedua yaitu United States.

Negara	Oktober	November	Desember
Indonesian	91.3%	85.89%	95.7%
United States	3.89%	3.93%	1.19%
Russia	3.11%	9.31%	3.0%
United Kingdom	0.11	0.06%	
Singapore	0.92%	0.17%	0.03%
Germany	0.32%	0.17%	
None	0.36%	0.46%	0.08%

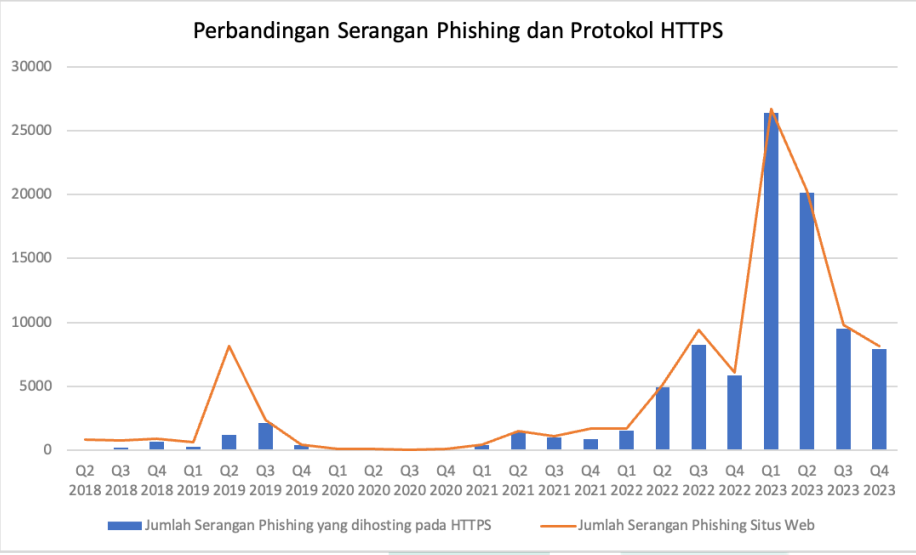
Industri Sasaran Phishing



Sektor industri yang paling ditargetkan untuk serangan phishing pada kuartal keempat yaitu media sosial sebesar 64,34%, yang selanjutnya diikuti pada posisi kedua yaitu lembaga keuangan sebesar 20,58%. Pada beberapat kuartal terakhir, sektor media sosial menempati posisi tertinggi daripada sector lembaga keuangan. Hal ini harus diwaspadai juga oleh masyarakat Indonesia dalam menggunakan media sosial.

Serangan Phishing Pada Situs Web yang Terenkripsi

Berdasarkan data yang terkumpul pada dashboard IDADX, dilakukan analisa terhadap situs phishing yang menggunakan protocol HTTPS.



Pada saat ini situs web phishing yang digunakan kebanyakan menggunakan protocol HTTPS. Kami melakukan perbandingan antara jumlah serangan phishing pada situs web dan situs web yang menggunakan protokol HTTPS. Dapat dilihat dari tahun 2021, jumlah protocol HTTPS lebih banyak digunakan hingga kuartal kedua tahun 2023.
Berdasarkan dari grafik tersebut, sejak Q3 tahun 2019 hingga Q4 tahun 2023 jumlah serangan phishing pada situs web yang menggunakan protokol HTTPS mengalami peningkatan. Hal ini menunjukkan bahwa, situs web yang terenkripsi banyak digunakan untuk phishing dan memiliki celah untuk diretas.

Tentang IDADX

Indonesia Anti-Phishing Data Exchange (IDADX) didirikan pada tahun 2021 dibawah kepengurusan Pengelola Nama Domain Internet Indonesia (PANDI). IDADX adalah sebuah inisiasi untuk meningkatkan keamanan siber nasional dengan memfasilitasi respons global terhadap kejahatan internet di sektor pemerintah, penegakan hukum, industri, dan komunitas internet.

Pada saat ini kami bekerjasama dengan para Registrar PANDI untuk memerangi adanya phishing. Kami tentunya tidak hanya berhenti sampai disini, kami akan mengembangkan dashboard phishing ini dengan menambah sumber data kami dan bekerjasama dengan pihak lainnya agar data yang kami miliki terpercaya dan terbaru.

IDADX mengelola situs web publik https://www.idadx.id dimana masyarakat bisa melaporkan url yang menggunakan domain .id sebagai phishing. Selain itu, laporan seputar phishing juga dapat dilaporkan melalui email helpdesk@pandi.id.