

Waspada penipuan melalui Instagram: centang biru dan verifikasi palsu



Instagram adalah salah satu platform media sosial yang terbesar saat ini, dengan pengguna dengan lebih dari 2 miliar pengguna aktif bulanan, namun tidak sedikit pula para penipu memanfaatkan celah untuk melakukan penipuan, mulai dari pemalsuan identitas dengan centang biru, hingga jebakan “verified badge” yang menjanjikan status sosial media.

1. Penipuan Jasa Verifikasi Instagram

Modus ini menawarkan jasa “centang biru” dengan iming-iming:

- Proses cepat (24-72 jam) dengan biaya beragam dari ratusan hingga jutaan rupiah
- Klaim bisa mendapatkan “koneksi” dengan tim Instagram.
- Penggunaan identitas palsu sebagai agen resmi dari Meta

Faktanya verifikasi Instagram hanya bisa di peroleh melalui proses resmi dari aplikasi dengan syarat:

- Akun anda mewakili sosok terkenal
- Memiliki kepentingan pencarian yang tinggi (orang banyak yang mencari nama anda)
- Akun autentik, lengkap, dan unik.

2. Pemalsuan Akun Resmi

Penipu biasanya membuat akun dengan:

- Logo dan nama mirip dengan instansi resmi (@bankbca_official vs @bank_bca_official)
- Centang biru palsu yang diperoleh dengan menggunakan karakter Unicode atau edit foto
- Konten yang disalin dari akun asli dan mengedit konten tersebut untuk mendapatkan korban.

3. Modus “Instagram Partnership Program”

Penipuan baru-baru ini mengirim pesan pribadi yang mengklaim seperti “Selamat! Anda terpilih untuk Instagram Partnership Program” dan “Dapatkan penghasilan dengan memposting konten” lalu korban diminta untuk membayar biaya pendaftaran atau data kartu kredit.

Modus Penipuan Lain yang harus diwaspadai

Selain modus centang biru, platform Instagram juga diwarnai oleh berbagai bentuk penipuan lainnya yang memanfaatkan fitur dan dinamika sosial dalamnya. Modus seperti “giveaway” atau undian palsu merupakan penipuan yang cukup populer. Penipu membuat konten yang menjanjikan hadiah yang mahal seperti gadget terbaru, uang tunai dalam jumlah yang besar, atau sepeda motor, dengan syarat mengikuti akun tertentu, menandai teman korban, dan yang paling krusial adalah mentransfer sejumlah uang untuk biaya administrasi atau pengiriman. Setelah uang di transfer, akun tersebut biasanya menghilang atau memblokir korban.

Modus lain yang lebih canggih adalah penipuan melalui fitur “close friends” (teman dekat yang ada pada Instagram), pelaku berusaha menyusup ke daftar teman dekat korban, baik dengan memanfaatkan kelemahan keamanan atau membangun hubungan secara perlahan. Setelah dianggap “dekat”, mereka dapat dengan leluasa mengirim tautan phising yang seolah-olah video atau informasi pribadi, atau meminjam sejumlah uang dengan alasan yang mendesak. Keakraban palsu inilah yang membuat korban lengah.

Cara Melindungi diri dari Penipuan Instagram

Pertama, verifikasi keaslian palsu dengan cara periksa username dengan teliti, akun resmi biasanya tidak menggunakan angka/karakter aneh.

Kedua, tips keamanan umum, jangan pernah membagikan kode OTP/2FA ke siapapun, kemudian Aktifkan two factor-authentication di pengaturan yang ada di instagram, Waspada terhadap tautan pendek (bit.ly, tinyurl) yang di kirim via DM, dan langsung verifikasi melalui saluran resmi jika ada keraguan.

Ketiga, jika menemui penipuan laporan akun tersebut melalui fitur report yang ada pada instagram, screenshot semua bukti percakapan dan transfer, laporan ke polisi melalui patroli siber atau cyber crime, dan laporan ke bank untuk membekukan transaksi jika memungkinkan.

Dampak Hukum dan Regulasi

Pelaku penipuan Instagram dapat dikenai pasal-pasal:

- Pasal 378 KUHP tentang Penipuan (ancaman pidana 4 tahun penjara)
- Pasal 28 UU ITE tentang Keterangan Palsu (pidana 6 tahun dan dana 1 miliar)
- Pasal 263 KUHP tentang Pemalsuan Surat (pidana 6 tahun)

Data dan Tren Penipuan Instagram di Indonesia

Berdasarkan laporan Kaspersky Lab (2023), Indonesia termasuk 10 besar negara dengan serangan phishing melalui media sosial tertinggi di Asia Tenggara. Sementara Laporan Keamanan Siber Kominfo (2024) mencatat peningkatan 45% laporan penipuan digital melalui Instagram dibanding tahun sebelumnya.

Sumber Referensi:

1. Instagram Help Center. About Verified Badges. Diakses dari <https://help.instagram.com>
2. Kementerian Komunikasi dan Informatika (Kominfo). Laporan Keamanan Siber 2024.
3. Meta Transparency Center. Community Standards Enforcement Report.
4. Kaspersky Lab. (2023). Social Media Phishing Report.
5. Kepolisian Republik Indonesia. Modus Penipuan Digital 2024.
6. Asosiasi E-Commerce Indonesia (idEA). Panduan Keamanan Transaksi Online.