PEMERINTAH KABUPATEN KUTAI TIMUR
Dinas Komunikasi, Informatika, Statistik dan Persandian
Tim Tanggap Insiden Siber — KUTIM-CSIRT

PANDUAN TEKNIS

Kesiapsiagaan Menghadapi Phishing

Panduan praktis bagi pegawai di lingkungan Pemerintah Kabupaten Kutai Timur untuk mengenali, menghindari, dan menanggapi upaya pengelabuan (*phishing*).

Nomor Dokumen	**KUTIM-CSIRT/PANDUAN/004/2026**
Versi	**1.0**
Klasifikasi	**TERBUKA — untuk umum**
Tanggal Terbit	**Mei 2026**
Disusun oleh	**Tim Tanggap Insiden Siber Kabupaten Kutai Timur (KUTIM-CSIRT)**

KUTIM-CSIRT
csirt.kutaitimurkab.go.id · csirt@kutaitimurkab.go.id

Kata Pengantar

Pengelabuan atau *phishing* merupakan salah satu bentuk gangguan keamanan siber yang paling sering dijumpai dan paling sering berhasil. Berbeda dengan serangan yang menyasar kelemahan perangkat lunak, phishing menyasar manusia — memanfaatkan rasa percaya, kelalaian, dan tekanan waktu untuk memperoleh data, kata sandi, atau akses yang seharusnya terlindungi.

Pegawai di lingkungan pemerintah daerah menjadi sasaran yang menarik bagi pelaku karena akses yang dimilikinya terhadap surel kedinasan, aplikasi layanan, dan data masyarakat. Satu akun yang terkecoh dapat menjadi pintu masuk bagi gangguan yang lebih luas terhadap sistem Perangkat Daerah.

Atas dasar itu, Tim Tanggap Insiden Siber Kabupaten Kutai Timur (KUTIM-CSIRT) menyusun panduan ini sebagai acuan ringkas bagi seluruh pegawai. Panduan disajikan tanpa istilah teknis yang rumit, agar dapat langsung dipahami dan diterapkan dalam pekerjaan sehari-hari.

Kepada semua pihak yang telah memberikan masukan dalam penyusunan panduan ini, kami sampaikan penghargaan dan terima kasih. Saran perbaikan untuk edisi berikutnya dapat disampaikan melalui kanal resmi KUTIM-CSIRT.

Sangatta, Mei 2026

Tim Tanggap Insiden Siber
Kabupaten Kutai Timur

KUTIM-CSIRT

Daftar Isi

BAB 1

Pendahuluan

1.1 Latar Belakang

Phishing adalah upaya pengelabuan yang dilakukan untuk mencuri data pribadi, kredensial akun, atau uang dengan cara menyamar sebagai pihak yang terpercaya. Pelaku biasanya mengirim pesan yang tampak resmi — seolah berasal dari pimpinan, bank, penyedia layanan, atau instansi pemerintah — lalu mengarahkan korban untuk menyerahkan informasi rahasia atau membuka tautan dan lampiran berbahaya.

Phishing merupakan salah satu pintu masuk gangguan keamanan yang paling sering dimanfaatkan. Penanganan insiden di berbagai instansi menunjukkan bahwa banyak kebocoran data dan pengambilalihan akun bermula dari satu pesan pengelabuan yang berhasil. Pegawai pemerintah menjadi sasaran karena akses yang dimilikinya terhadap surel kedinasan, aplikasi layanan, serta data masyarakat. Karena phishing menyasar manusia dan bukan perangkat lunak, kewaspadaan setiap pegawai menjadi lapis pertahanan yang menentukan.

1.2 Maksud dan Tujuan

Panduan ini disusun dengan maksud meningkatkan kesiapsiagaan pegawai dalam menghadapi upaya pengelabuan. Tujuannya adalah:

- menyamakan pemahaman tentang apa itu phishing dan bagaimana cara kerjanya;
- membekali pegawai dengan kemampuan mengenali ciri pesan dan tautan yang mencurigakan;
- menyediakan sikap dan langkah pencegahan yang dapat langsung diterapkan;
- menjelaskan langkah penanganan dan cara pelaporan apabila terlanjur menjadi korban.

1.3 Ruang Lingkup

Panduan ini mencakup pengenalan phishing melalui berbagai kanal, ciri-ciri pesan dan tautan yang patut dicurigai, sikap aman dalam bekerja, serta langkah penanganan bila terlanjur terkecoh. Panduan ini bersifat umum dan edukatif; rincian teknis yang dapat disalahgunakan sengaja tidak dicantumkan. Pengamanan tingkat sistem dan jaringan dibahas dalam dokumen lain dan dikoordinasikan dengan KUTIM-CSIRT.

1.4 Sasaran Pengguna

Dokumen ini ditujukan bagi seluruh pegawai, termasuk Aparatur Sipil Negara, di lingkungan Perangkat Daerah Pemerintah Kabupaten Kutai Timur, tanpa memandang jabatan atau latar belakang teknis. Pimpinan Perangkat Daerah juga dapat menggunakan panduan ini untuk membangun kesadaran keamanan di lingkungan kerjanya.

1.5 Dasar Acuan

- Peraturan Presiden Nomor 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik;
- Peraturan Badan Siber dan Sandi Negara mengenai penyelenggaraan keamanan siber dan pembentukan Tim Tanggap Insiden Siber pada instansi pemerintah;
- Keputusan Bupati Kutai Timur Nomor 555/K.557/2024 tentang Pembentukan Tim Tanggap Insiden Siber Kabupaten Kutai Timur.

BAB 2

Mengenal Phishing

Memahami cara kerja phishing adalah langkah pertama untuk tidak terkecoh olehnya. Pelaku selalu mengandalkan satu hal yang sama: membuat korban bertindak terburu-buru sebelum sempat berpikir.

Pada dasarnya, phishing bekerja dengan menyamar. Pelaku meniru pihak yang dipercaya korban, lalu menyampaikan alasan yang tampak masuk akal agar korban menyerahkan informasi atau melakukan tindakan tertentu. Tujuan pelaku umumnya adalah memperoleh kata sandi dan kode masuk akun, mengambil data pribadi, mengelabui korban agar mentransfer uang, atau menanam program berbahaya pada perangkat korban melalui tautan dan lampiran. Upaya pengelabuan dapat menyasar siapa saja, namun sering pula diarahkan khusus kepada pejabat atau pegawai tertentu dengan pesan yang dirancang seolah-olah berkaitan dengan tugasnya.

Pengelabuan dapat datang melalui beragam kanal. Pegawai perlu mengenali masing-masing kanal tersebut.

No	Kanal Pengelabuan	Uraian Singkat
1	**Surel** (*email*)	Kanal yang paling umum. Pelaku mengirim surel yang tampak resmi, memuat tautan ke halaman palsu atau lampiran berbahaya, dan sering menyaru sebagai pimpinan, rekan kerja, atau penyedia layanan.
2	**Pesan singkat dan WhatsApp**	Pesan berisi tautan atau permintaan data yang dikirim melalui SMS atau aplikasi pesan. Sering memakai nama dan foto profil yang menyerupai pejabat atau instansi resmi.
3	**Telepon**	Penelepon menyaru sebagai petugas bank, instansi, atau dukungan teknis, lalu menggiring korban menyebutkan kata sandi, kode satu kali pakai, atau data penting lainnya.
4	**Situs web palsu**	Halaman yang dibuat menyerupai situs resmi, termasuk halaman masuk aplikasi. Data yang dimasukkan korban langsung diterima pelaku. Alamatnya biasanya mirip namun tidak sama dengan yang asli.

CATATAN

Sebuah upaya pengelabuan kerap menggabungkan beberapa kanal sekaligus — misalnya surel yang disusul telepon untuk meyakinkan korban. Apa pun kanalnya, polanya tetap sama: menyamar sebagai pihak terpercaya dan menekan korban agar bertindak cepat. Mengenali pola inilah, bukan menghafal setiap modus, yang menjadi bekal utama kewaspadaan.

BAB 3

Ciri-ciri Pesan dan Tautan Phishing

Sebagian besar upaya pengelabuan dapat dikenali dari tanda-tanda yang berulang. Bila satu atau lebih ciri berikut ditemukan pada sebuah pesan, perlakukan pesan itu sebagai mencurigakan.

No	Ciri yang Patut Dicurigai	Penjelasan
1	**Pengirim mencurigakan atau menyaru**	Alamat pengirim tidak sesuai dengan instansi yang diakuinya, memakai domain yang mirip namun keliru, atau nama tampilan yang sengaja dibuat menyerupai pihak resmi.
2	**Desakan atau ancaman**	Pesan menuntut tindakan segera dengan dalih batas waktu, sanksi, atau akun yang akan diblokir. Desakan ini sengaja diciptakan agar korban tidak sempat memeriksa kebenarannya.
3	**Tautan yang disamarkan**	Teks tautan terlihat resmi, tetapi alamat tujuan sebenarnya berbeda dan mengarah ke situs palsu. Alamat asli dapat berbeda jauh dari yang ditampilkan.
4	**Lampiran yang tidak diharapkan**	Pesan menyertakan berkas yang tidak diminta atau tidak relevan dengan pekerjaan. Lampiran semacam ini dapat memuat program berbahaya.
5	**Permintaan kata sandi, kode, atau data pribadi**	Pesan meminta kata sandi, kode satu kali pakai, nomor rekening, atau data pribadi lain. Instansi resmi tidak pernah meminta informasi rahasia melalui pesan atau telepon.
6	**Kejanggalan bahasa atau tata letak**	Terdapat salah eja, tata bahasa yang kaku, sapaan yang umum dan tidak menyebut nama, atau tampilan logo dan tata letak yang tidak rapi dibanding pesan resmi yang biasa diterima.

Tautan adalah bagian yang paling sering dimanfaatkan dalam phishing, sehingga perlu diperiksa sebelum diklik. Pada komputer, arahkan kursor ke tautan tanpa menekannya, lalu perhatikan alamat tujuan yang muncul; pada telepon genggam, tekan tahan tautan untuk menampilkan alamatnya. Cermati apakah nama domain sungguh sesuai dengan instansi atau layanan yang dimaksud, karena pelaku kerap memakai alamat yang hanya berbeda satu atau dua huruf. Bila alamat tampak janggal, tidak dikenali, atau tidak sesuai isi pesan, jangan dibuka. Tautan yang meragukan dapat diperiksa lebih lanjut dengan cara yang dijelaskan pada Bab 4.

BAB 4

Sikap Aman dan Pencegahan

Mencegah phishing tidak memerlukan keahlian khusus, melainkan kebiasaan yang konsisten. Langkah-langkah berikut sebaiknya diterapkan setiap kali menerima pesan, terutama yang meminta tindakan atau informasi.

- **Jangan tergesa-gesa.** Berhenti sejenak setiap kali sebuah pesan menuntut tindakan segera. Desakan adalah ciri khas pengelabuan; pesan resmi yang sah dapat menunggu untuk diperiksa.
- **Jangan klik tautan atau buka lampiran yang meragukan.** Bila ragu terhadap asal atau isi pesan, jangan membuka tautan maupun lampirannya.
- **Verifikasi melalui kanal resmi.** Bila pesan mengaku berasal dari pimpinan, rekan, bank, atau instansi, konfirmasikan langsung melalui nomor atau kanal resmi yang sudah dikenal — bukan melalui kontak yang tercantum dalam pesan itu sendiri.
- **Ketik sendiri alamat resmi di peramban.** Untuk masuk ke aplikasi layanan atau perbankan, ketik alamatnya secara langsung di peramban, jangan mengikuti tautan dari pesan.
- **Aktifkan autentikasi dua faktor.** Pada akun surel dan aplikasi layanan, aktifkan autentikasi dua faktor agar akun tetap terlindungi meskipun kata sandi terlanjur diketahui pihak lain.
- **Laporkan pesan mencurigakan.** Sampaikan pesan yang dicurigai kepada KUTIM-CSIRT agar dapat ditelusuri dan rekan kerja lain dapat diingatkan.

Untuk membantu pemeriksaan, tautan yang meragukan dapat dicek melalui fitur Cek Phishing pada situs KUTIM-CSIRT di alamat **csirt.kutaitimurkab.go.id/cek-phishing**. Fitur ini memberi penilaian awal atas tingkat risiko suatu tautan, namun tetap perlu disertai sikap waspada dan akal sehat.

Daftar periksa berikut dapat digunakan untuk menilai kesiapsiagaan diri secara mandiri. Pegawai memberi tanda pada butir yang telah menjadi kebiasaan, dan menjadikan butir yang belum terpenuhi sebagai perhatian.

No	Butir Kesiapsiagaan	Sudah
A. SIKAP SAAT MENERIMA PESAN		
1	Tidak terburu-buru menanggapi pesan yang mendesak.	☐
2	Memeriksa alamat pengirim sebelum mempercayai isi pesan.	☐
3	Memeriksa alamat tujuan tautan sebelum mengkliknya.	☐
4	Tidak membuka lampiran yang tidak diharapkan.	☐
B. VERIFIKASI DAN AKSES		
5	Mengonfirmasi permintaan melalui kanal resmi yang dikenal.	☐
6	Mengetik sendiri alamat resmi aplikasi di peramban.	☐
7	Tidak pernah menyebutkan kata sandi atau kode kepada siapa pun.	☐
C. PENGAMANAN AKUN		
8	Autentikasi dua faktor aktif pada surel dan aplikasi layanan.	☐
9	Kata sandi panjang, unik, dan tidak dipakai ulang.	☐

No	Butir Kesiapsiagaan	Sudah
D. PELAPORAN		
10	Mengenali kanal pelaporan KUTIM-CSIRT.	☐
11	Bersedia melaporkan pesan mencurigakan yang diterima.	☐
12	Mengetahui langkah yang harus diambil bila terlanjur terkecoh.	☐

BAB 5

Bila Terlanjur Menjadi Korban dan Pelaporan

Terkecoh oleh phishing dapat terjadi pada siapa saja dan bukan hal yang perlu disembunyikan. Yang menentukan besarnya dampak adalah kecepatan dan ketepatan tindakan setelah disadari.

5.1 Langkah Penanganan Cepat

Apabila Anda menyadari telah mengklik tautan phishing, memasukkan data pada halaman palsu, atau menyerahkan informasi kepada pihak yang mencurigakan, segera lakukan langkah berikut:

1. Segera ganti kata sandi akun yang terdampak dari perangkat lain yang terpercaya, dan ganti pula kata sandi akun lain yang memakai kata sandi serupa.
2. Bila menyangkut keuangan, seperti data perbankan atau transaksi, segera hubungi bank atau penyedia layanan melalui nomor resmi untuk memblokir atau mengamankan rekening.
3. Dokumentasikan bukti: simpan pesan, tangkapan layar, alamat tautan, serta catat waktu kejadian dan tindakan yang sempat dilakukan.
4. Laporkan kejadian kepada KUTIM-CSIRT agar dapat ditelusuri dan dampaknya dibatasi, serta beri tahu atasan bila menyangkut akun atau data kedinasan.

> **PENTING**
>
> Jangan menunda pelaporan karena malu atau khawatir disalahkan. Penanganan yang cepat dapat mencegah kerugian yang jauh lebih besar, baik bagi diri sendiri maupun bagi instansi. Jangan pula menghapus pesan atau bukti, karena masih diperlukan untuk penelusuran.

5.2 Pelaporan kepada KUTIM-CSIRT

KUTIM-CSIRT menerima laporan dugaan phishing dan insiden keamanan siber dari seluruh pegawai Perangkat Daerah maupun masyarakat. Saat melapor, sertakan informasi sejelas mungkin: isi dan asal pesan, waktu kejadian, tindakan yang sudah dilakukan, serta bukti pendukung. Pelaporan dapat dilakukan melalui kanal berikut.

Kanal Pelaporan Insiden — KUTIM-CSIRT

Formulir daring	**csirt.kutaitimurkab.go.id/lapor**
Surel	**csirt@kutaitimurkab.go.id**
Telepon	**(0549) 2021207 — pada jam kerja**
Lacak laporan	**csirt.kutaitimurkab.go.id/lacak-tiket**

PENUTUP

Penutup

Phishing akan terus berkembang mengikuti kebiasaan dan teknologi yang digunakan masyarakat. Namun, sekuat apa pun upaya pengelabuan dirancang, ia selalu bertumpu pada kelengahan manusia. Karena itu, kewaspadaan setiap pegawai — bukan perangkat lunak semata — merupakan pertahanan yang paling menentukan.

Langkah-langkah dalam panduan ini sederhana dan dapat segera menjadi kebiasaan. KUTIM-CSIRT terbuka untuk membantu Perangkat Daerah melalui pembekalan, pendampingan, maupun penanganan insiden. Panduan ini akan ditinjau secara berkala dan diperbarui sesuai perkembangan ancaman serta masukan dari para pengguna.

PERNYATAAN DOKUMEN

Dokumen ini diterbitkan oleh Tim Tanggap Insiden Siber Kabupaten Kutai Timur (KUTIM-CSIRT) di bawah Dinas Komunikasi, Informatika, Statistik dan Persandian Kabupaten Kutai Timur. Dokumen berklasifikasi TERBUKA dan boleh disebarluaskan di lingkungan pemerintah maupun masyarakat untuk tujuan peningkatan keamanan siber.

— SELESAI —