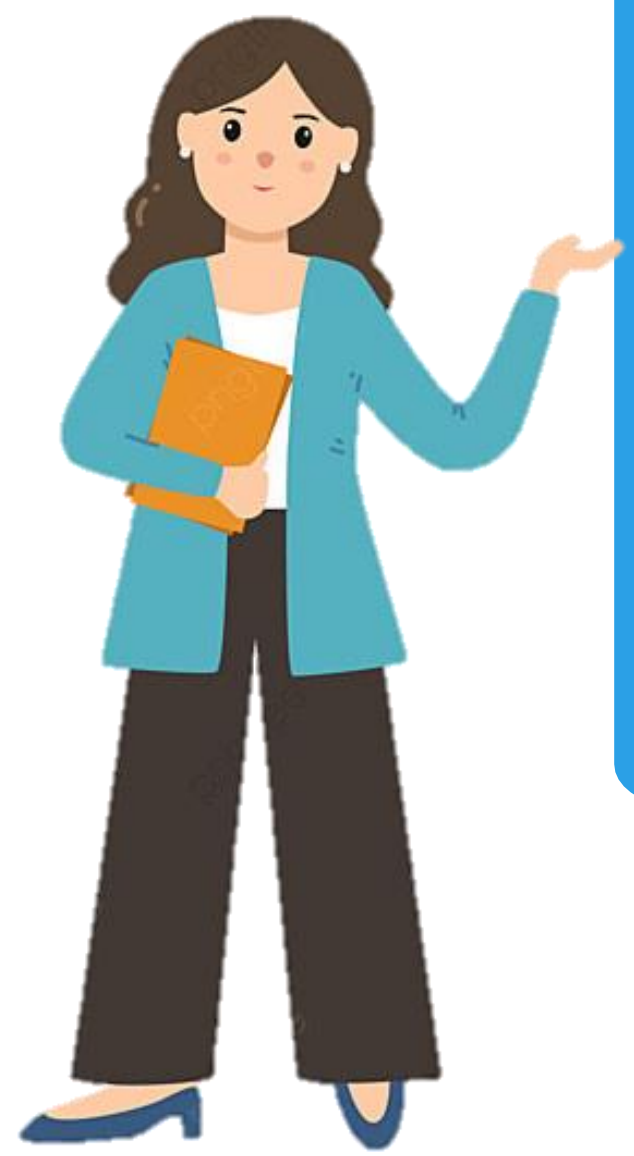




PANDUAN PENANGANAN INSIDEN **SERANGAN PHISING**

Dinas Komunikasi dan Informatika Kota Batam

PENDAHULUAN



Serangan phishing adalah serangan yang dilakukan untuk menipu /memancing korban agar mau mengklik tautan serta menginput informasi kredensial seperti username dan password

Cara kerja phishing umumnya dilakukan melalui penggunaan email palsu mengatasnamakan admin, atau melalui situs web palsu yang sangat mirip dengan situs web yang asli

TUJUAN

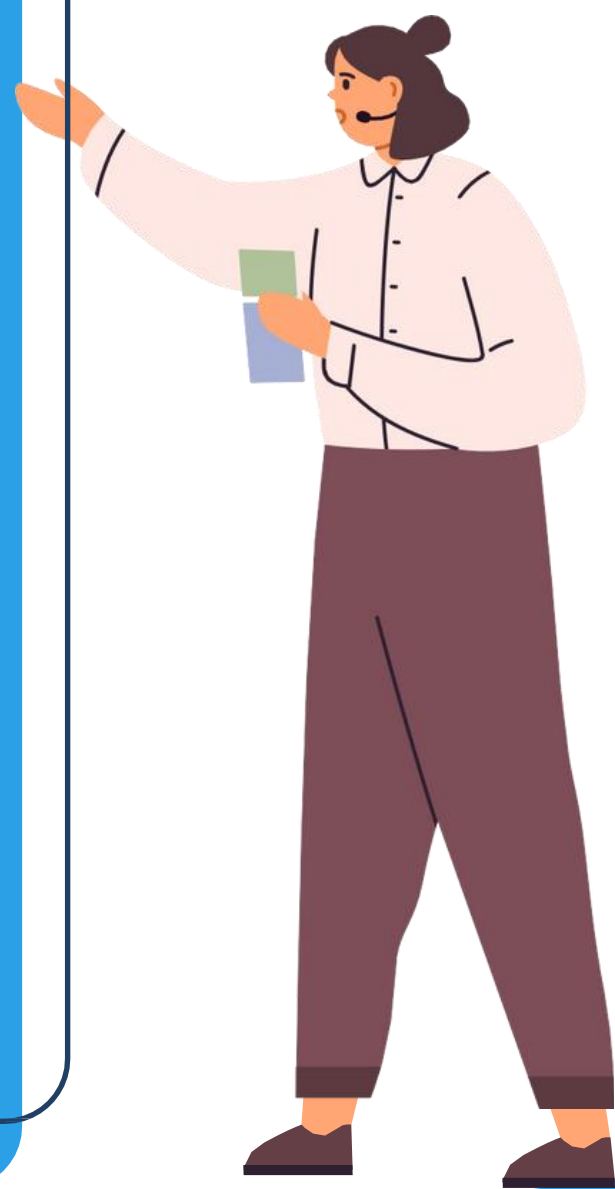
Tujuan panduan ini dimaksudkan untuk membantu organisasi memahami tentang penanganan seerangan pishing



RUANG LINGKUP

Panduan ini berisi langkah-langkah yang harus diambil apabila terjadi serangan phishing, yang dimulai dari tahap persiapan sampai dengan tahap pembuatan laporan dari penanganan serangan

Panduan ini dapat dijadikan acuan bagi semua individu atau tim (administrator, pengelola TI, tim respon insiden keamanan komputer) yang bertanggung jawab untuk mencegah, mempersiapkan atau menangani serangan phishing

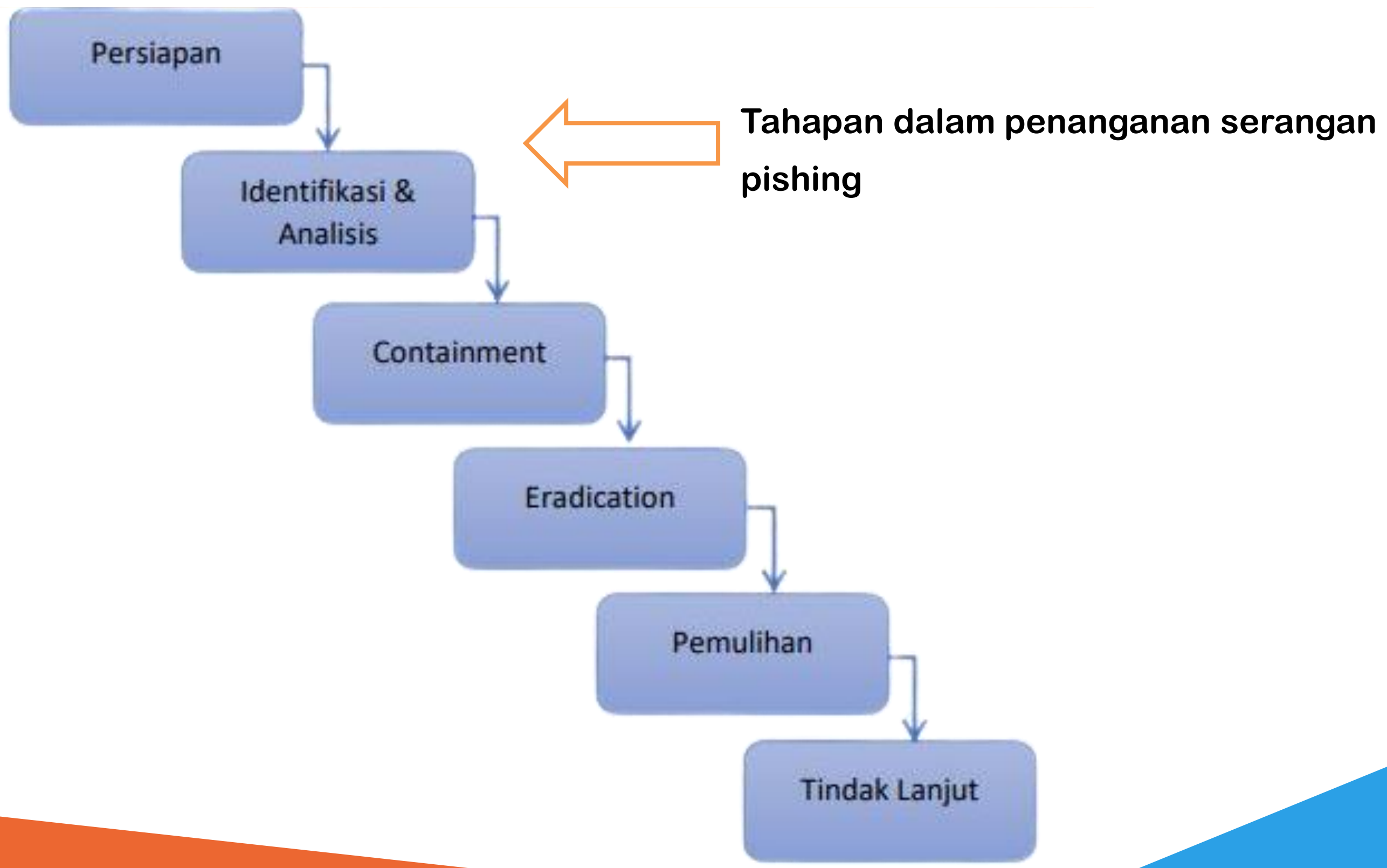


PROSEDUR PENANGANAN INSIDEN PISHING

Penanganan serangan phishing ditujukan untuk mencapai hal-hal sebagai berikut



PROSEDUR PENANGANAN INSIDEN PISHING



PROSEDUR

Pada tahap ini bertujuan untuk memulihkan kembali halaman web kepada keadaan semula

1. Membuat daftar semua domain sah yang dimiliki organisasi
2. Mempersiapkan satu buah halaman website untuk memperingatkan pengguna tentang terjadinya serangan phishing
3. Mempersiapkan formulir untuk informasi laporan penyalahgunaan domain
4. Membangun kontak dengan pihak-pihak terkait, seperti perusahaan hosting, penyedia domain, penyedia jasa email, Nasional CERT
5. Meningkatkan kesadaran terhadap serangan phishing, diantaranya :

Tidak mengklik link yang mencurigakan

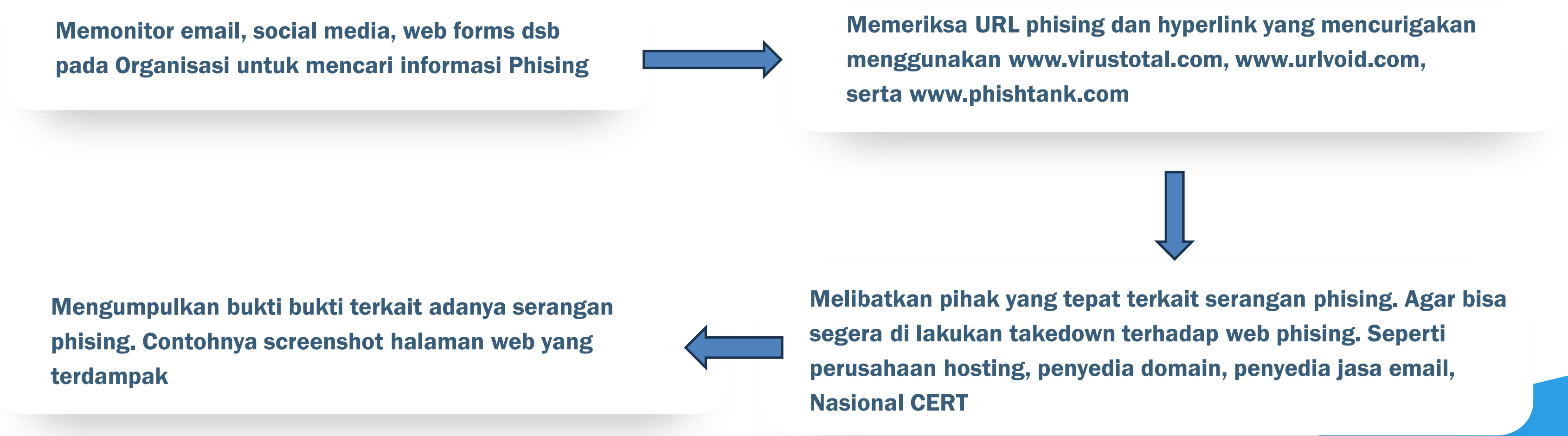
Tidak memasukkan username dan password pada situs web yang alamatweb nya meragukan

Merubah penulisan alamat email yang dipublish, dari bentuk @ menjadi "at" untuk menghindari menjadi target email phishing

Menggunakan Anti Virus yang memiliki fitur Anti Phising

IDENTIFIKASI DAN ANALISIS

Tujuan dari proses identifikasi adalah untuk mendeteksi adanya insiden serangan phishing, menentukan ruang lingkup, dan melibatkan pihak-pihak yang tepat dalam menangani serangan phishing



CONTAINMENT

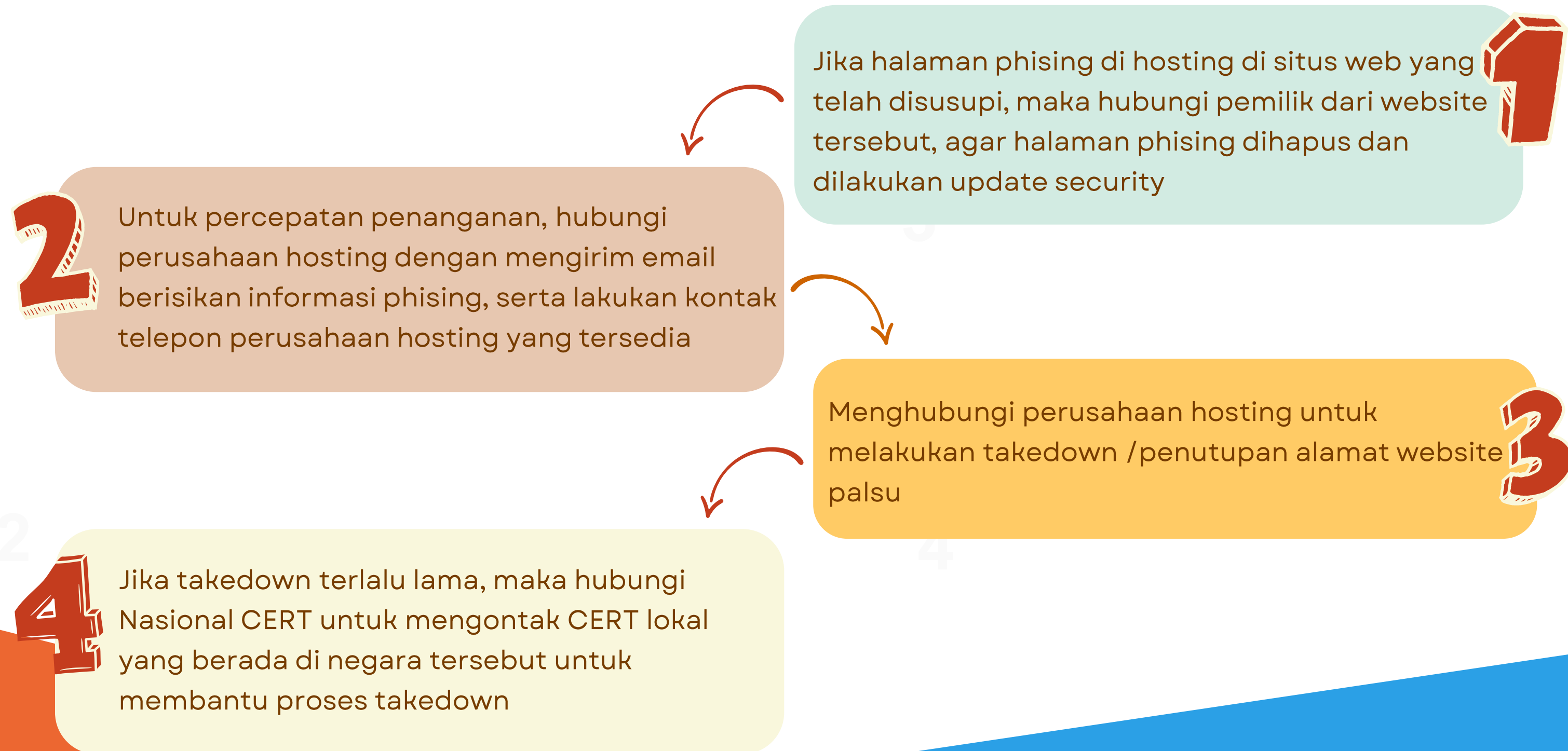
Setelah dipastikan bahwa memang benar telah terjadi serangan phishing, maka dilakukan proses mitigasi serangan, agar tidak terjadi kerusakan lebih dalam



- 1** Menyebarkan URL phishing dan konten dari email phishing pada pihak spamreporting website, misalnya www.phishtank.com
- 2** Menginformasikan serangan phishing kepada pengguna, agar pengguna mengetahui dan tidak terkena dampak dari serangan tersebut
- 3** Memeriksa source code dari website phishing, jika menggunakan gambar dari website yang anda miliki, anda dapat mengganti gambar dengan tampilan "PHISING WEBSITE"

ERADICATION

Proses ini bertujuan untuk mengambil tindakan dalam menghentikan serangan phishing. Prosedur untuk melakukan proses ini dapat dilakukan dengan cara berikut



PEMULIHAN

Pemulihan merupakan tahap untuk mengembalikan seluruh sistem bekerja normal seperti semula



TINDAK LANJUT

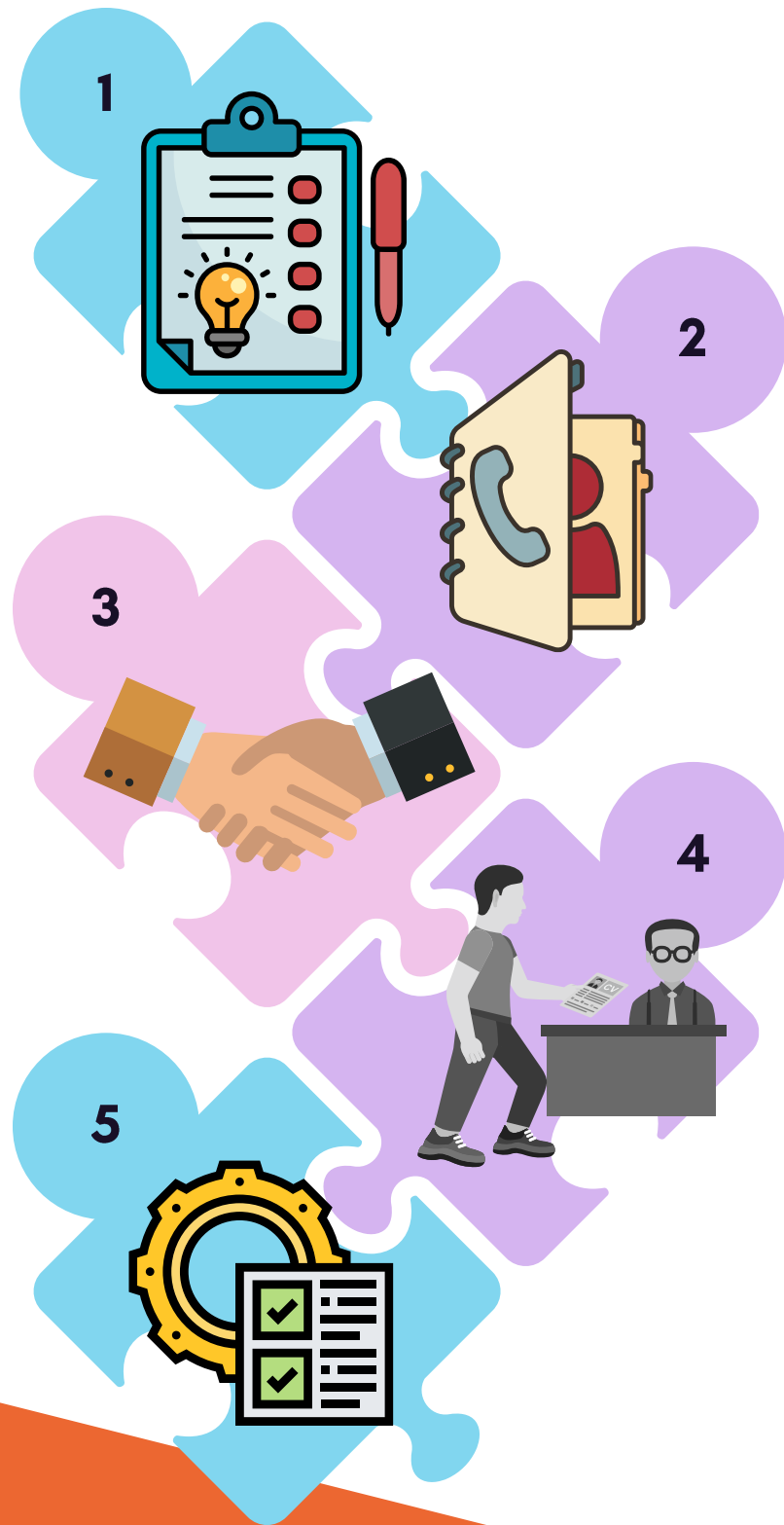
Tahap ini adalah fase di mana semua dokumentasi kegiatan yang dilakukan dicatat sebagai referensi untuk di masa mendatang

Tujuan

- 1** Pelaporan, membuat laporan mengenai langkah-langkah dan hasil yang telah didapatkan pada penanganan serangan phising
- 2** Mengambil pelajaran dan membuat rekomendasi untuk mencegah terjadi lagi

TINDAK LANJUT

Prosedur



- 1 Menyempurnakan langkah-langkah respon, prosedur penanganan serangan yang diambil selama insiden agar kedepannya dapat menangani insiden secara lebih cepat dan efisien
- 2 Memperbaharui daftar kontak yang dimiliki, disertai catatan cara paling efektif untuk menghubungi setiap pihak yang terlibat
- 3 Berkolaborasi dengan tim hukum jika diperlukan tindakan hukum
- 4 Membuat dokumentasi dan laporan terkait penanganan serangan Phising
- 5 Membuat evaluasi dan rekomendasi



PANDUAN PENANGANAN INSIDEN **SERANGAN PHISING**

Dinas Komunikasi dan Informatika Kota Batam