

Lindungi Diri dengan Keselamatan Siber

Penceramah: Helmy Hanyff Bin Hairudin Ruzaili

INI IKAN APA?





SIAPAKAH SAYA?

HELMY HANYFF BIN HAIRUDIN RUZAILI

Universiti Sultan Azlan Shah

Master of Science in Cybersecurity

- **Certified Information Security Awareness Manager (CISAM)**
- **SIMATIC Service 2 in the TIA Portal (TIA-SERV2) (TIA-SERV2)**
- **Certified Information Security Manager (ikut budget huhu)**
- **Certified Penetration Tester (ikut budget huhu)**
- **Certified Ethical Hacker (ikut budget huhu)**

Hobi: Suka menung sambil rendam bihun sambil menung

WWW.MAYBANK2U.COM

WWW.MAYBANK2U.COM

WWW.MAYBANK2U.COM

ADAKAH KITA SELAMAT?





Apa Itu Serangan Phishing?

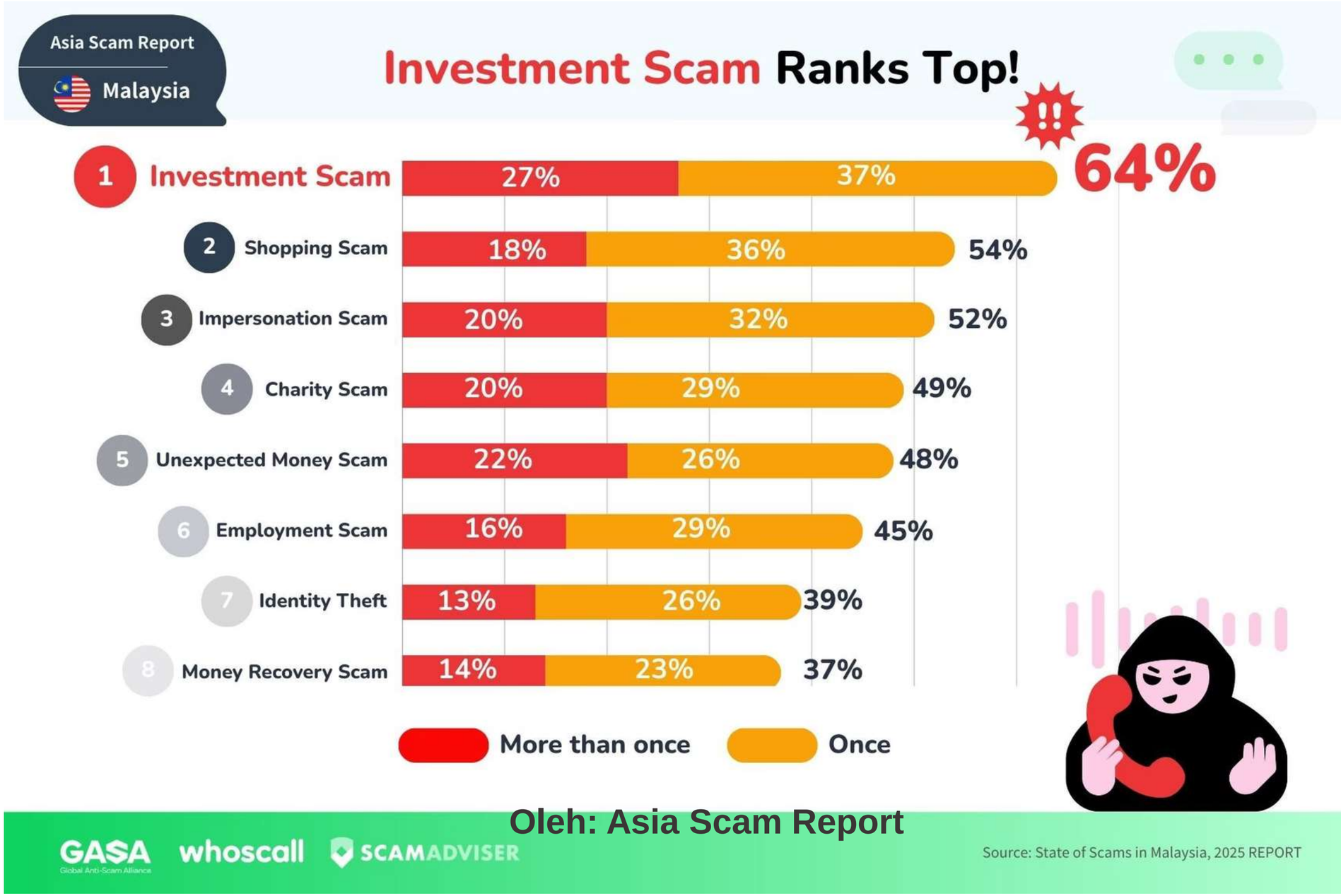
Penipuan Siber Berbahaya

- Phishing ialah penipuan siber yang cuba mencuri maklumat sensitif seperti kata laluan, nombor akaun bank, dan data kewangan penting.

Penyamaran Licik

- Penyerang menyamar sebagai entiti dipercayai seperti bank, pembekal, atau rakan kongsi perniagaan melalui e-mel atau mesej palsu yang kelihatan sah.

STATISTIC



Oleh: Asia Scam Report



Jangan Jadi Mangsa Phishing

Satu klik boleh membawa kepada bencana. Berhati-hati dengan setiap e-mel yang anda terima.

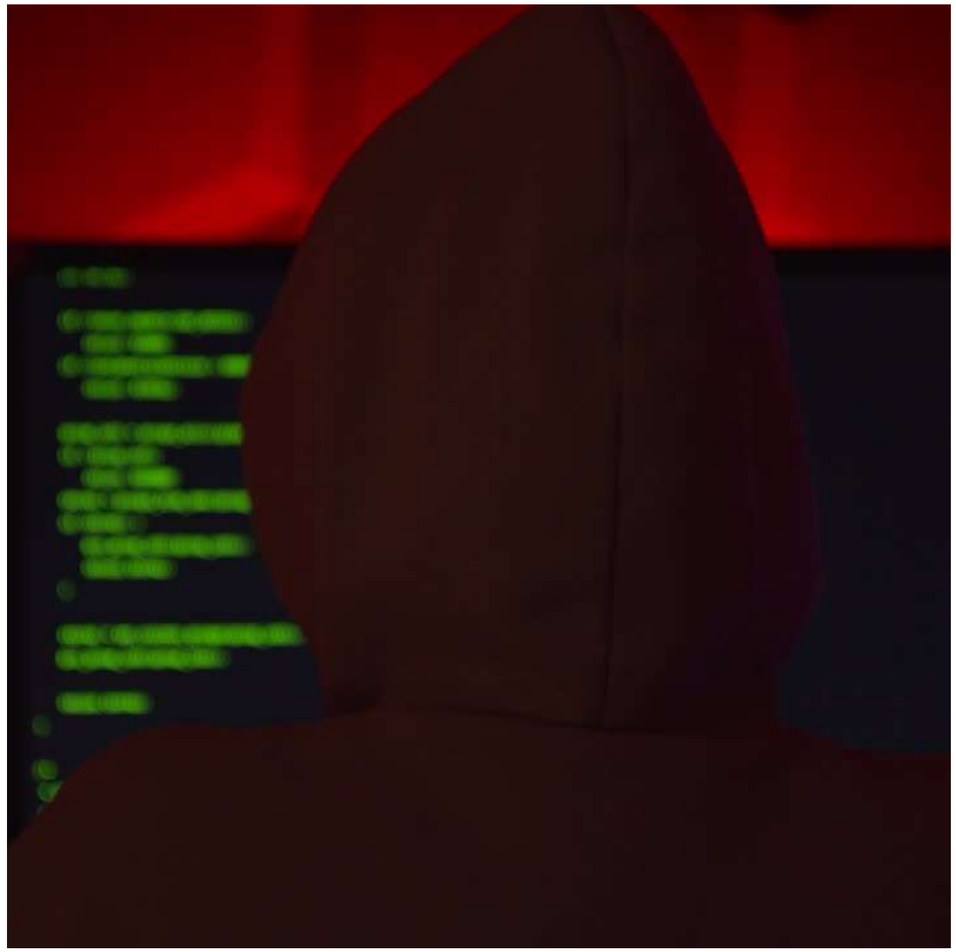
Mengapa Industri Perikanan Terancam?

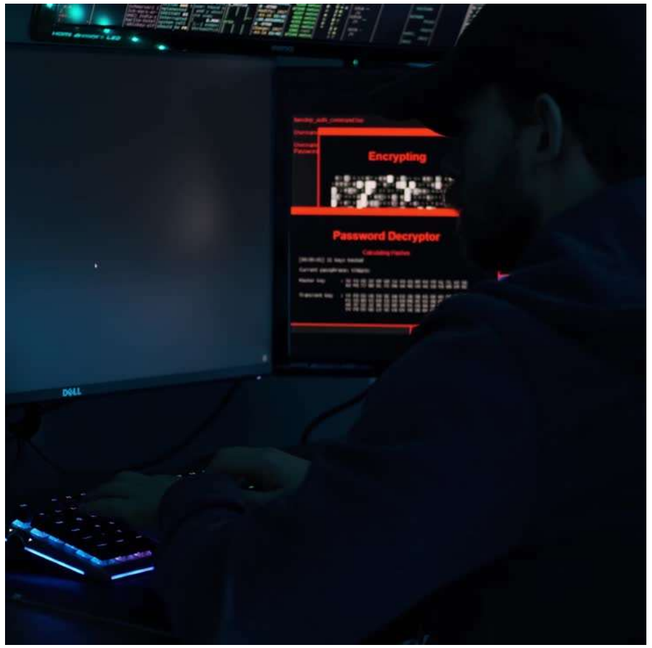
Pergantungan Digital Meningkat

- Banyak operasi perikanan kini bergantung sepenuhnya pada sistem digital untuk pengurusan stok ikan, pelacakan penghantaran, pemprosesan pesanan, dan transaksi kewangan harian.

Kesan Serangan Phishing

- Kehilangan data pelanggan dan pembekal yang sensitif
- Gangguan operasi yang melumpuhkan aktiviti harian
- Kerugian kewangan yang boleh mencecah ratusan ribu ringgit





DEMO 1

Keselamatan bermula dengan sikap berhati-hati.

Taktik Phishing Paling Lazim

Mesej Mendesak Dengan Ancaman

Mesej yang mencipta kepanikan dengan ancaman penutupan akaun, denda berat, atau tindakan undang-undang jika anda tidak bertindak dengan cepat.

Pautan ke Laman Web Palsu

Pautan yang membawa anda ke laman web palsu yang menyerupai portal rasmi jabatan perikanan, bank, atau platform e-dagang yang anda gunakan.



Tanda-tanda Serangan Phishing

1

Salam Yang Tidak Biasa atau Terlalu Umum

E-mel yang menggunakan sapaan seperti "Pelanggan Yang Dihormati" atau "Pengguna" tanpa menyebut nama anda secara spesifik patut disyaki.

2

Kesalahan Ejaan dan Tatabahasa

Mesej yang penuh dengan kesalahan bahasa, ejaan yang salah, atau ayat yang janggal menunjukkan ia mungkin penipuan.

3

Alamat E-mel atau URL Yang Meragukan

Periksa alamat e-mel pengirim dengan teliti. Contoh: "support@perlkanan.com" berbanding "support@perikanan.gov.my" - perhatikan perbezaan halus.

4

Permintaan Maklumat Secara Mendesak

Organisasi sah tidak akan meminta maklumat peribadi, kata laluan, atau butiran kewangan melalui e-mel dengan nada mendesak.



Perkogsian Keselamatan

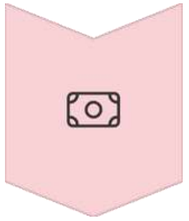
Jika ragu-ragu, hubungi organisasi tersebut secara langsung melalui nombor telefon rasmi mereka - jangan guna nombor yang tertera dalam e-mel mencurigakan itu!

Kesan Serangan Phishing Terhadap Perikanan



Kecurian Data Pelanggan dan Pembekal

Maklumat pelanggan, harga pembekal, dan butiran kontrak yang sensitif boleh jatuh ke tangan pesaing atau penjenayah siber.



Penipuan Kewangan

Pemindahan wang ke akaun palsu yang menyebabkan kerugian kewangan langsung kepada syarikat anda.



Gangguan Bekalan dan Penghantaran

Sistem logistik yang terjejas boleh menyebabkan kelewatan penghantaran hasil laut segar, mengakibatkan kerugian produk dan pelanggan.

Kes 1: Serangan Phishing di Syarikat Perikanan XYZ



Hari 1: Serangan Bermula

Penyerang menyamar sebagai pembekal utama dan menghantar invois palsu.

1

2

Hari 2: Pembayaran Dibuat



Jabatan kewangan memindahkan RM500,000 ke akaun bank palsu tanpa pengesahan telefon.



Hari 3: Penipuan Terbongkar

3

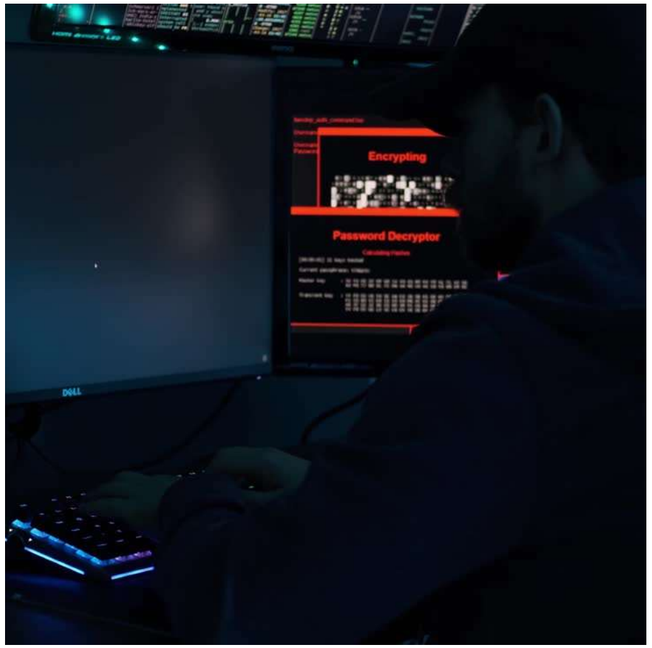
Pembekal sebenar menghubungi untuk menuntut bayaran yang tertunggak.

4

Minggu 1: Pemulihan



Operasi terhenti selama seminggu untuk siasatan dan pemulihan sistem keselamatan.



DEMO 2

Phishing berkembang setiap hari, kewaspadaan harus berganda.

SOFTWARE YANG BOLEH MEMBANTU

- GOOGLE LENS
- NORDVPN CHECKER
- MY DIGITAL ID
- CHATGPT



Teknik Melindungi Diri dan Organisasi Anda

Periksa Sebelum Klik

- Sentiasa sahkan alamat e-mel pengirim dan URL pautan dengan teliti sebelum mengklik apa-apa pautan atau memuat turun lampiran.

Jangan Kongsi Maklumat Sensitif

- Jangan sekali-kali berikan maklumat peribadi, kata laluan, atau butiran kewangan melalui e-mel, walaupun ia kelihatan sah.

Gunakan Pengesahan Dua Faktor (MFA)

- Aktifkan MFA untuk semua akaun penting - ini menambah lapisan keselamatan tambahan walaupun kata laluan anda dicuri.

Kemas Kini Perisian Keselamatan

- Pastikan antivirus, firewall, dan sistem operasi sentiasa dikemas kini dengan tampalan keselamatan terkini.

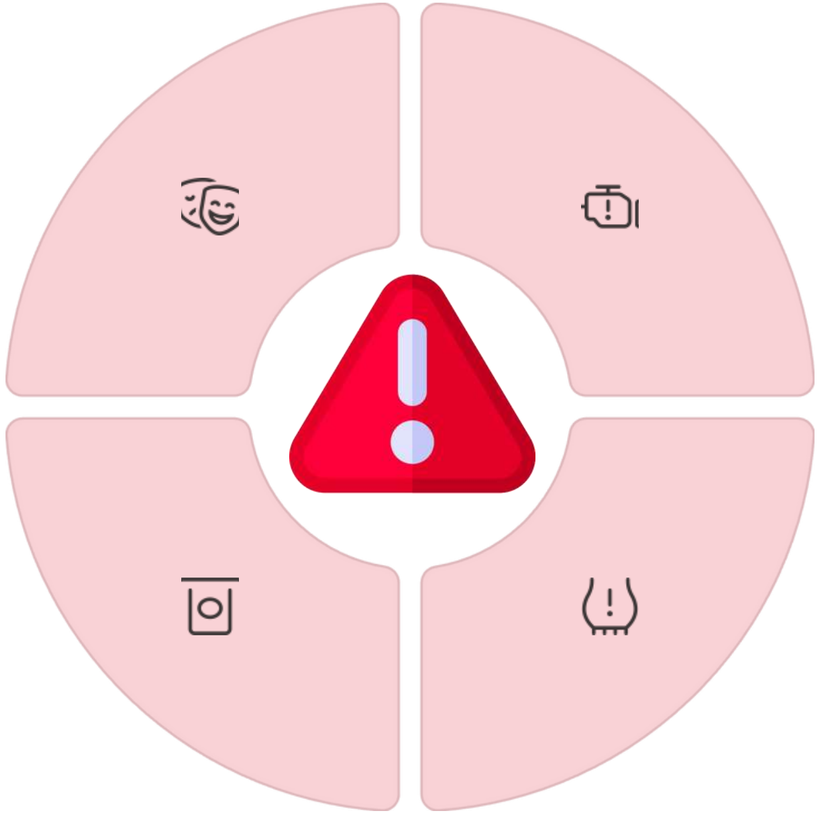
Empat P Penting Mengenal Phishing

Pretend (Bermuka)

Penyerang menyamar sebagai organisasi dipercayai seperti bank, agensi kerajaan, atau rakan perniagaan anda.

Pay (Bayar)

Minta bayaran melalui cara yang sukar dijejaki seperti pemindahan wang, cryptocurrency, atau kad hadiah.



Problem (Masalah)

Mereka cipta masalah palsu atau krisis mendesak untuk menakut-nakutkan dan memanipulasi emosi anda.

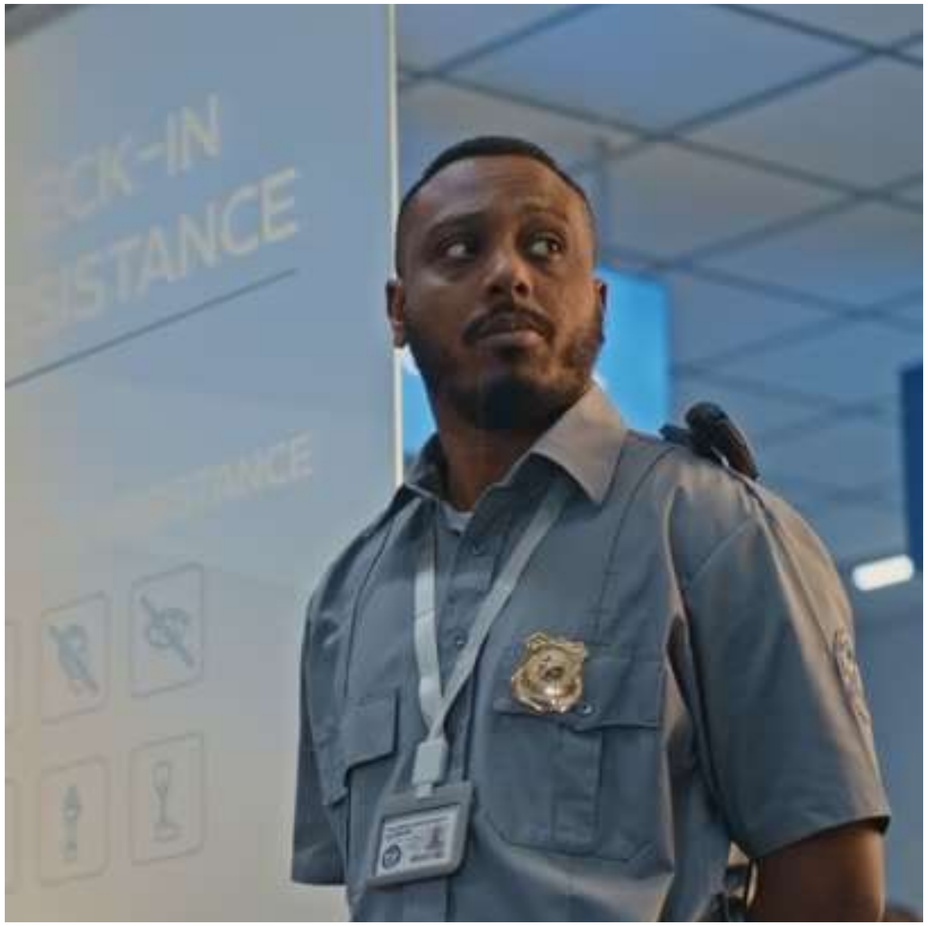
Pressure (Tekanan)

Tekan anda untuk bertindak segera tanpa fikir panjang, menggunakan taktik seperti "Akaun anda akan ditutup dalam 24 jam!"



4P: Senjata Anda Melawan Phishing

Contoh Protokol Keselamatan Pembayaran



01

Terima Permintaan Pembayaran

Sebarang permintaan pembayaran diterima melalui e-mel atau mesej.

02

Jangan Buat Pembayaran Segera

Jangan terus membuat pembayaran berdasarkan e-mel atau mesej sahaja, walaupun ia kelihatan mendesak.

03

Sahkan Melalui Panggilan Telefon

Hubungi pembekal atau pihak yang membuat permintaan melalui nombor telefon rasmi yang anda sudah ada dalam rekod.

04

Gunakan Saluran Rasmi Syarikat

Sahkan butiran pembayaran melalui portal rasmi syarikat atau sistem pengurusan yang sedia ada.

Apa Yang Perlu Dilakukan Jika Terkena Phishing?

1

Jangan Panik - Putuskan Sambungan

- Segera putuskan sambungan internet untuk mengelakkan kerosakan lanjut. Matikan WiFi atau cabut kabel rangkaian dengan cepat.

2

Tukar Semua Kata Laluan

- Tukar segera kata laluan untuk semua akaun yang mungkin terjejas, terutama akaun bank, e-mel, dan sistem pengurusan syarikat.

3

Laporkan Kejadian

- Maklumkan kepada jabatan IT, pengurus, dan pihak berkuasa siber seperti CyberSecurity Malaysia atau polis untuk tindakan susulan.

Tindakan Pantas Adalah Kunci

Setiap minit yang berlalu selepas serangan phishing boleh mengakibatkan lebih banyak kerosakan. Bertindak pantas tetapi dengan bijak!

Pelaburan Dalam Latihan Adalah Pelaburan Dalam Keselamatan

Pekerja yang terlatih adalah pertahanan terbaik anda terhadap serangan phishing dan ancaman siber yang lain.





ADA APA-APA LAGI?

Identiti anda aset, jangan serahkan kepada penipu.

Kesimpulan

Phishing: Ancaman Nyata Kepada Industri Perikanan

- Serangan phishing bukan lagi sekadar ancaman teori - ia adalah bahaya nyata yang boleh melumpuhkan operasi perikanan, menyebabkan kerugian kewangan yang besar.

Kesedaran dan Pencegahan Adalah Kunci

- Dengan kesedaran yang tinggi, latihan berterusan, dan amalan keselamatan yang baik, kita boleh mengurangkan risiko menjadi mangsa penipuan siber ini dengan ketara.

Bersama Kita Lebih Kuat

- Industri perikanan yang bersatu dalam menghadapi ancaman siber akan lebih berdaya tahan. Kongsi pengetahuan, laporkan serangan, dan lindungi satu sama lain.



90%
Serangan Boleh Dicegah

3x
Risiko Meningkat



Bersama Melawan Phishing

Emel palsu boleh menipu mata, tetapi bukan mereka yang berjaga-jaga.