CYBERSÉCURITÉ

NOUS SOMMES TOUS CONCERNÉS

PDF

Sur ordinateur, smartphone ou internet, adopte les bons réflexes !



IFSB

cases.lu
Cyberworld Awareness and Security Enhancement Services
LUXEMBOURG

CHAMBRE DES METIERS
Luxembourg

Cybersécurité n°2 : Phishing

N’importe qui peut vous envoyer un courriel en se faisant passer pour un autre ! Cela n’est pas beaucoup plus compliqué que de mettre un faux nom d’expéditeur au verso d’une enveloppe.

Le phishing ou hameçonnage, est une technique utilisant principalement les courriers électroniques et visant à obtenir des informations personnelles (identifiants, mots de passe, données bancaires...).
L’arnaqueur, tente de “pêcher les informations de sa victime”, en se faisant passer pour un organisme de confiance (par exemple une banque), via un site web falsifié. Ce type d’attaque s’adresse principalement à des particuliers, mais des données vitales de l’entreprise peuvent également être visées.

Nous vous invitons à regarder cette vidéo du CASES sur le sujet du phising:
https://youtu.be/FhsnUiFVv0k

Voici 4 réflexes à adopter face aux tentatives d'hameçonnage / phishing

1. **N’AYEZ PAS UNE CONFIANCE AVEUGLE DANS LE NOM DE L’EXPÉDITEUR.**
   Soyez attentif à tout indice mettant en doute l’origine de l'e-mail, notamment si le message comporte une pièce jointe ou des liens.
   En cas d’incohérence, doute, contactez votre interlocuteur par un canal de communication différent (ex: par téléphone)

2. **MÉFIEZ-VOUS DES PIÈCES JOINTES !**
   Elles peuvent contenir des virus ou des logiciels espions

3. **NE RÉPONDEZ JAMAIS À UNE DEMANDE D’INFORMATIONS CONFIDENTIELLES.**
   Les demandes d’informations confidentielles (mots de passe, code PIN, coordonnées bancaires, *etc*.), ne sont jamais faites par e-mail . En cas de doute, demandez par téléphone à votre correspondant de confirmer.

4. **FAITES ATTENTION AUX CARACTÈRES ET LA SYNTAXE.**
   Un texte dans une mauvaise qualité, des caractères accentués, des liens suspects, trahissent souvent une tentative d’arnaque.

Cybersécurité n°2 : Phishing

Qualquer pessoa lhe pode enviar um e-mail fazendo-se passar por outra pessoa! Isso não é muito mais complicado do que colocar um nome de remetente falso no verso de um envelope.

O *phishing* é uma técnica que utiliza principalmente o correio eletrónico e que visa obter informações pessoais (credenciais, palavras-passe, dados bancários ...).
O criminoso tenta "pescar informações da sua vítima", fazendo-se passar por um organismo de confiança (por exemplo, um banco), através de um website falso. Este tipo de ataque é dirigido, principalmente, a particulares, mas os dados vitais da empresa e do negócio também podem ser visados.

Convidamos a assistir a este vídeo da CASES sobre o phishing:
https://youtu.be/FhsnUiFVv0k

4 conselhos a adotar face às tentativas de phishing

1. **NÃO CONFIE CEGAMENTE NO NOME DO REMETENTE.**
   Preste atenção a quaisquer indícios que possam questionar a origem do e-mail, nomeadamente se a mensagem tiver um anexo ou links.
   Em caso de inconsistência ou dúvida, contacte o seu interlocutor através de um canal de comunicação diferente (ex:, por telefone)

2. **DESCONFIE DOS ANEXOS!**
   podem conter vírus ou programas-espiões (spyware)

3. **NÃO RESPONDA NUNCA A UM PEDIDO DE INFORMAÇÕES CONFIDENCIAIS.**
   Os pedidos de informações confidenciais (palavras-passe, código PIN, dados bancários, *etc*.), não são enviados nunca por e-mail. Em caso de dúvida, contacte ao seu interlocutor por telefone para confirmar.

4. **PRESTE ATENÇÃO AOS CARATERES E À SINTAXE.**
   Um texto de má qualidade, carateres acentuados, links suspeitos, denunciam frequentemente uma tentativa de golpe.

Cybersécurité n°2 : Phishing

CYBERSÉCURITÉ
NOUS SOMMES TOUS CONCERNÉS

Heutzutage kann jeder unter falschem Namen E-Mails versenden! Das ist ungefähr so kompliziert wie auf der Rückseite eines Briefumschlags einen falschen Absender anzugeben.

Phishing bezeichnet eine Technik, bei der vorwiegend über E-Mails versucht wird, an personenbezogene Daten wie Benutzernamen, Passwörter, Bankdaten usw. zu gelangen. Der Betrüger gibt sich dabei über eine gefälschte Website als vertrauenswürdige Instanz (beispielsweise als Bank) aus und versucht, „Informationen seines Opfers zu stehlen“. Derartige Betrugsversuche zielen in erster Linie auf Privatpersonen ab, allerdings können auch wichtige Daten von Unternehmen ins Visier der Betrüger gelangen.

Ausführliche Erläuterungen zum Thema Phishing enthält dieses Video der CASES:
https://youtu.be/FhsnUiFVv0k

Nachfolgend vier Verhaltensweisen, mit denen Sie sich vor Phishing-Versuchen schützen können:

1. **VERTRAUEN SIE ABSENDERN VON E-MAILS NICHT BLIND!**
   Achten Sie aufmerksam auf jegliche Indizien für die Herkunft der E-Mail, insbesondere sofern Dateianhänge oder Links enthalten sind.
   Nehmen Sie bei jeglichen Unstimmigkeiten oder Zweifeln über einen anderen Kommunikationskanal (z.B. Telefon) Kontakt mit dem Absender auf.

2. **SEIEN SIE VORSICHTIG MIT DATEIANHÄNGEN!**
   Dateianhänge können Viren oder Spyware enthalten.

3. **GEBEN SIE NIEMALS VERTRAULICHE INFORMATIONEN PREIS!**
   Anfragen zur Einholung vertraulicher Informationen (Passwörter, PIN-Codes, Bankdaten usw.) werden niemals per E-Mail versendet. Klären Sie die Angelegenheit im Zweifelsfall telefonisch mit dem Absender.

4. **ACHTEN SIE AUF DAS SCHRIFTBILD UND DEN SATZBAU!**
   Schlecht geschriebene Texte, hervorgehobene Schriftzeichen und verdächtige Links sind häufig Anzeichen für Betrugsversuche.

Cybersécurité n°2 : Phishing

IFSB

cases.lu
Cyberworld Awareness and Security Enhancement Services
LUXEMBOURG

CHAMBRE DES METIERS
Luxembourg