Was ist Phishing?

Phisher fischen nach wertvollen Informationen.

Mit gefälschten E-Mails versuchen sie:

- **Passwörter oder Kreditkartendaten zu stehlen.**
- **einen Computervirus zu verbreiten.**

STOP | THINK | CONNECT™

Schützen Sie sich!

- Beantworten Sie niemals E-Mail-Anfragen nach Passwörtern, Sicherheitscodes, PIN-Codes, etc.
- Öffnen Sie nur E-Mail-Anhänge von Absendern, denen Sie vertrauen.
- Seien Sie misstrauisch bei E-Mails, die “umgehendes Handeln” erfordern.
- Trauen Sie keiner E-Mail mit einer allgemeinen Anrede, wie “Lieber Kunde” oder “Sehr geehrte Damen und Herren”.
- Seien Sie misstrauisch gegenüber E-Mails mit Rechtschreib- und Grammatikfehlern.
- Behandeln Sie E-Mails von einem bekannten Absender, aber ungewöhnlichen E-Mail-Adresse mit Vorsicht.
- Ein Link in einer E-Mail? Fahren Sie mit der Maus darüber und finden Sie heraus, wo der Link wirklich hinführt.

Haben Sie eine Phishing-Mail oder eine Phishing-Webseite entdeckt? Helfen Sie mit, das Internet sicherer zu machen! Melden Sie die Phishing-Adresse an:
https://www.antiphishing.ch

Zusammen für ein sicheres Internet!
https://www.stopthinkconnect.ch

UNIVERSITÉ DE GENÈVE
UNIVERSITÉ DE FRIBOURG UNIVERSITÄT FREIBURG
UNIVERSITÄT LIECHTENSTEIN
b UNIVERSITÄT BERN
Hes·SO GENÈVE Haute Ecole Spécialisée de Suisse occidentale
FFHS Fernfachhochschule Schweiz Zürich | Basel | Bern | Brig Mitglied der SUPSI
Universität Konstanz
HSR HOCHSCHULE FÜR TECHNIK RAPPERSWIL FHO Fachhochschule Ostschweiz
Lucerne University of Applied Sciences and Arts HOCHSCHULE LUZERN FH Zentralschweiz
SWISS INTERNET SECURITY ALLIANCE
EUROPEAN CYBER SECURITY MONTH
Internet Society Switzerland Chapter
global IP action
open systems
APWG www.apwg.org
SWITCH
STOP | THINK | CONNECT™
eBanking aber sicher!

Was ist Phishing?

Der Begriff “Phishing” kommt vom englischen Wort für “fischen”: “to fish”. Laut Definition bezeichnet Phishing den Versuch, über gefälschte Emails oder Webseiten sensitive Daten, wie Passwörter oder Kreditkartendaten, zu stehlen. Das Opfer verliert dabei zweifach: Daten und Geld!

Phishing-Angriffe starten mit einer E-Mail. Eine Phishing-Mail kann ein verlockendes Angebot unterbreiten oder sofortige Handlung Ihrerseits verlangen, um Sie dazu zu bringen

- ein gefälschtes Formular auszufüllen.
- einen Link zu einer gefälschten Webseite zu klicken.
- einen infizierten Anhang zu öffnen.

Häufig benutzen Phisher dabei Logos bekannter Unternehmen, um Ihr Vertrauen zu gewinnen.

Seien Sie misstrauisch bei E-Mails, die “umgehendes Handeln” erfordern.

Mit unterschiedlichen Methoden versuchen Phisher, Sie unter Druck zu setzen und zu einer impulsiven und nicht durchdachten Handlung zu verleiten. Wird Ihnen via E-Mail mitgeteilt, Ihr Konto werde gelöscht, wenn Sie nicht umgehend Ihr Passwort ändern, verfallen Sie nicht in Panik. Denken Sie vielmehr daran: Beantworten Sie niemals E-Mail-Anfragen nach Passwörtern, Sicherheitscodes, PIN-Codes etc.

Trauen Sie keiner E-Mail mit einer allgemeinen Anrede, wie “Lieber Kunde” oder “Sehr geehrte Damen und Herren”.

Phishing-Angriffe zielen im Allgemeinen nicht auf eine einzelne Person ab – ein und dieselbe E-Mail wird an tausende Adressen geschickt. Deshalb beginnen die meisten Phishing-Mails mit einer allgemeinen Anrede. Ihre Bank und Ihr bevorzugter Online-Shop kennen aber Ihren Namen und werden Sie in einer E-Mail persönlich anreden.

Ein Link in einer E-Mail? Fahren Sie mit der Maus darüber und finden Sie heraus, wo der Link wirklich hinführt.

Die meisten Phishing-Mails nutzen gefälschte Links, um Sie auf eine gefälschte Webseite zu locken oder einen Virus auf Ihrem Computer zu installieren. Diese Links sind üblicherweise sehr lang. Um keinen Verdacht zu erregen, nutzen Phisher Kurzlinks oder überschreiben den Link mit einem anderen Text. Auf diese Weise ist der wirkliche Link nicht sichtbar – fahren Sie mit der Maus darüber (nicht klicken!) und der wahre Zielort des Links wird sich zeigen.

Sind Sie auf eine Phishing-Mail hereingefallen?

Keine Angst – so etwas kann jedem passieren. Je nachdem, welche Informationen Sie preisgegeben haben, haben Sie verschiedene Möglichkeiten:

- Nehmen Sie Kontakt zu Ihrer Bank auf und sperren Sie Ihre Kreditkarte und ggf. Ihr Konto.
- Informieren Sie Unternehmen oder Institution, von denen die E-Mail vermeintlich versendet wurde.
- Ändern Sie alle Passwörter, die gestohlen worden sein könnten. Wenn zum Beispiel Ihr E-Mail-Passwort „gephisht“ wurde, überlegen Sie, ob der Phisher mit dem Zugriff auf Ihre E-Mails noch weitere Passwörter besitzen könnte.
- Beobachten Sie all Ihre Online-Konten wie Amazon, Facebook etc. und melden Sie verdächtige Vorfälle. Es kann nicht schaden, die Passwörter zu ändern!
- Stellen Sie sicher, dass Ihr Antivirenprogramm auf dem neusten Stand ist und starten Sie einen Virenscan auf Ihrem Computer.

Beantworten Sie niemals E-Mail-Anfragen nach Passwörtern, Sicherheitscodes, PIN-Codes, etc.

Weder Ihre Bank noch irgendein anderes seriöses Unternehmen wird Sie darum bitten, Ihre Passwörter, Sicherheitscodes oder PIN-Codes per E-Mail zu senden. Sie sind sich nicht sicher, ob die E-Mail echt oder gefälscht ist? Überprüfen Sie den Absender, indem Sie:

- die Bank oder Firma anrufen.
- die Bank oder Firma persönlich besuchen.
- eine E-Mail an eine Ihnen bekannte Adresse schicken (antworten Sie NICHT auf die zweifelhafte E-Mail).

Öffnen Sie nur E-Mail-Anhänge von Absendern, denen Sie vertrauen.

Es gibt Dateien, die durch das blosse Öffnen einen Virus auf Ihrem Computer installieren können. Sie erhalten eine E-Mail mit einer Rechnung für etwas, das Sie nicht bestellt haben? Oder eine E-Mail mit einem Abholschein für ein überraschendes Paket? Phisher kennen Wege, das Öffnen des Anhangs unwiderstehlich zu machen. Behandeln Sie Dateien im Anhang von verdächtigen E-Mails mit Vorsicht – im Zweifel gilt: Die E-Mail ungeöffnet löschen.

Seien Sie misstrauisch gegenüber E-Mails mit Rechtschreib- und Grammatikfehlern.

Allgemeine Phishing-Angriffe setzen auf Quantität statt Qualität. Aus diesem Grund sind die meisten Phishing-Mails nicht sorgfältig formuliert. Einige beinhalten offensichtlich schlechte Übersetzungen, andere haben lediglich ein paar Rechtschreibfehler. Vergessen Sie nicht, dass Ihre Bank und die meisten Unternehmen Ihnen keine E-Mail mit fehlerhaftem Text schicken würden.

Behandeln Sie E-Mails von einem bekannten Absender, aber ungewöhnlichen E-Mail-Adresse mit Vorsicht.

Einige Phishing-Mails nutzen eine Tarnung, um zu Ihnen durchzukommen. Sie sehen das Logo Ihrer Bank oder Ihres bevorzugten Online-Shops – aber wurde die E-Mail von der Adresse gesendet, von der Bank und Online-Shop Sie üblicherweise kontaktieren? Vergleichen Sie die Absenderadresse mit denen, die Sie bereits kennen.

BEWARE OF THE PHISHING HOOK

Testen Sie Ihr Anti-Phishing-Wissen mit dem Phishing-Quiz von “eBanking – aber sicher!” auf:
https://www.ebas.ch/phishingtest

Haben Sie eine Phishing-Mail oder eine Phishing-Webseite entdeckt? Helfen Sie mit, das Internet sicherer zu machen! Melden Sie die Phishing-Adresse an:
https://www.antiphishing.ch

Zusammen für ein sicheres Internet!
https://www.stopthinkconnect.ch