

Gefahren im Internet



Begrüßung / Vorstellung

Roland Walter



- Seit 29 Jahren bei der Polizei Basel-Landschaft, davon
- 21 Jahre Sicherheitspolizei, zuletzt Leiter Polizeihauptposten Muttenz
- 6 Jahre Kriminalpolizei als Ermittler
- 6 Jahre Fliegender Einsatzleiter (Polizeihelikopter)
- Seit 2015 Präventionsbeauftragter/Mediensprecher



GEFÄLSCHTE RECHNUNGEN



Erfundene Rechtsanwälte und Inkassobüros versenden Rechnungen per E-Mail, für die es keinen Rechtsgrund gibt. Die betrügerischen E-Mails beinhalten Dateianhänge, die von den Empfängern geöffnet werden sollen. In diesen Dateianhängen befinden sich jedoch gefährliche Schad-Software.

TIPPS:

- Nicht alles glauben, was in E-Mails behauptet wird.
- Im Internet informieren, ob es den/die AbsenderIn wirklich gibt.
- Keine unbekanntem Dateianhänge öffnen.
- Betrügerische E-Mails nicht beantworten und löschen.



PHISING

Kriminelle versuchen an persönliche Zugangsdaten von Internet-nutzerInnen zu kommen. Dazu versenden sie gefälschte E-Mails oder Nachrichten, in denen dazu aufgefordert wird, auf einer Webseite persönliche Daten einzugeben. Die Websites sind Fälschungen, die geheimen Zugangsdaten wandern direkt an die BetrügerInnen.

TIPPS:

- Seriöse Unternehmen erfragen keine pers. Daten per E-Mail.
- Nie vertrauliche Daten auf Nachfrage im Internet bekannt geben.
- Verdächtige E-Mails löschen und keine darin enthaltenen Links klicken oder Dateianhänge öffnen.



ABO-FALLEN

Auf den ersten Blick kostenlose Angebote im Internet führen nach erfolgter Registrierung zu einem kostenpflichtigen Abo.

TIPPS:

- Auch im Internet hat niemand etwas zu verschenken!
- Wenn persönliche Daten verlangt werden:
Im Kleingedruckten nach Kostenhinweisen schauen.
- Vorsicht bei Gewinnspielen: Oft werden mit der Teilnahme unerwartete Kosten fällig.
- Nicht durch Rechnungen einschüchtern lassen und Hilfe bei einer Konsumentenschutz-Organisation holen.



BETRÜGERISCHER VERKAUF IM INTERNET



Betrüger bieten im Internet sehr günstige Produkte an. Oft sind Websites aufwändig gestaltet und wirken auf den ersten Blick seriös. Nach der Bezahlung, die vorab geleistet werden muss, folgt die Ernüchterung: Die Ware wird nicht geliefert, weil es sie gar nicht gibt. Das bezahlte Geld ist weg.

TIPPS:

- Sich über den Anbieter informieren
- Bei sehr günstigen Preisen skeptisch sein
- Sind auf der Seite keine Angaben über den Verkäufer zu finden: Nicht kaufen!
- Möglichst keine Waren im Voraus per Banküberweisung bezahlen, keine Käufe mit Bargeldtransferdiensten (z.B. Western Union, MoneyGram) tätigen.

Weitere Tipps

- Bankgeschäfte: Nach Logout immer Cache leeren, nur so lange wie nötig online sein, auf «https-Verbindung» achten.
- Nie auf «Link» klicken, Buchstaben von Hand eingeben
- Verdächtige Mails und Internetseiten an KOBİK weiterleiten

Aktuelle Fälle in Basel-Land

- SMS-Abo auf Pornoseiten
- Geldforderungen in sozialen Medien (z.B. Sextortion)
- Betrügerische Immobiliengeschäfte und Fahrzeugverkäufe
- Anruf von «Microsoft-Support»
- Trojaner «Bundespolizei»
- Spanische Klassen-Lotterie
- Verbotene Pornographie

https://www.melani.admin.ch/melani/de/home.html

Mele- und Analyse...

Bundesverwaltung MELANI

Startseite Übersicht Kontakt DE FR IT EN

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Melde- und Analysestelle
Informationssicherung MELANI

Aktuelle Gefahren Wie schütze ich mich? Dokumentation Meldeformular Über MELANI

Melde- und Analysestelle Informationssicherung MELANI



In der Melde- und Analysestelle Informationssicherung MELANI arbeiten Partner zusammen, welche im Umfeld der Sicherheit von Computersystemen und des Internets sowie des Schutzes der schweizerischen kritischen Infrastrukturen tätig sind.

Die Website von MELANI richtet sich an private Computer- und Internetbenutzer, sowie an kleinere und mittlere Unternehmen (KMU) der Schweiz. Viren und Würmer haben in der Vergangenheit bereits Millionen von Computern lahm gelegt. Die entstandenen Schäden wie Datenverlust oder Ausfall von Dienstleistungen waren riesig. Das muss nicht sein! Schützen Sie Ihre wertvollen Daten!

Informationen für:

- Privatanwender
- Unternehmen
- Webseitenbetreiber

Dokumentation

Die MELANI Halbjahresberichte erläutern die wichtigsten Tendenzen und Entwicklungen rund um Vorfälle und Geschehnisse in den Informations- und Kommunikationstechnologien (IKT). Mit Checklisten und Anleitungen können Sie in verschiedenen Themenbereichen Ihre Systeme sicherer machen.

125% 13:23 27.07.2015

Browser address bar: <https://www.cybercrime.admin.ch/kobik/de/home.html>

Navigation: Datei Bearbeiten Ansicht Favoriten Extras ?

Taskbar: Berufsschau Willkommen bei Forum Kr... Home Solutions D-Link D... Schweizerische Kriminalpr...

[Aktuell](#)
[Gefahren im Netz](#)
[Meldeformular](#)
[Warnmeldungen](#)
[Publikationen](#)
[Über uns](#)



Koordinationsstelle zur Bekämpfung der Internetkriminalität
 Service de coordination de la lutte contre la criminalité sur Internet
 Servizio di coordinazione per la lotta contro la criminalità su Internet
 Cybercrime Coordination Unit Switzerland

Willkommen auf der Site der Schweizerischen Koordinationsstelle zur Bekämpfung der Internetkriminalität (KOBIK).



Meldeformular

Melden Sie uns strafbare Inhalte und Verhalten im Internet via unserem Online-Meldeformular.

WARNUNG



Betrügerische Mails mit Absender fedpol

Aktuell sind E-Mails mit dem angeblichen Absender „Bundesamt für Polizei“ im Umlauf. >

Warnung: Kostenpflichtige Nummern und Hilfeforderung von gehacktem Facebook-Profil

Warnung: Spam-Mails mit Verlinkung auf eine gefälschte Webseite von fedpol

Augen auf!

Meldeformular

Browser address bar: <https://www.cybercrime.admin.ch/kobik/de/home/meldeformular/meldeformular.html>

Taskbar: 125% 13:18 27.07.2015

Lieber Kunde ,

Bitte beachten Sie, dass Ihre Apple ID wird in weniger als 48 Stunden ablaufen.
Es muss eine Prüfung durchzuführen Ihrer Daten, sonst Ihren Benutzernamen, werden vernichtet.

Klicken Sie einfach auf den unten stehenden Link und melden Sie sich mit Ihrer Apple-ID und Passwort.

Überprüfen Sie Ihren Account <<http://www.polskagazeta.ie/imgpart/>>

Apple-Kundendienst

Copyright 2015 iTunes, Inc. Alle Rechte vorbehalten.

Apple Inc. copyright © 2015 Infinite Loop, MS 98-DM, Cupertino, CA 95015

Alle Rechte vorbehalten / Informationsservice / Datenschutz / Meine Apple ID

**VON SITZ DES VIZE PRASIDENTEN
INTERNATIONALE PROMOTION-GEWINNZUTEILUNG**

Capitan Haya 53 Plz 3,
28020 Madrid, Spain.

ATTENTION: LOTO GEWINNER/IN
REFERENZNUMMER: JES5456010-ESP
BEARBEITUNGSNUMMER: JE88/00133/IPD/10
Oktober 2015

06.

(TRANSLATED COPY)

Wir sind erfreut ihnen mitteilen zu können, das die gewinnliste LOTTO PROGRAMM an 30.09.2015 Erschienen ist. Die offizielle liste der gewinner erschien am 6.10.2015, Ihr name wurde auf dem los mit dir nummer: 3120 4852 4450 und mit der seriennummern: 8119-04 registried. Die glucksnummer: 01-09-18-29-36, haben in der 3.kategorie gewonnen.

Sie sind damit gewinner von: 2.100,000.00 (NUR ZWEI MILLIONE EIN HUNDERT TAUSEND EURO.) Die summe ergibt sich einer gewinnausschuttung von 56.700,000.00 (SECHS UND FUNFZIG MILLIONE SIEBEN HUNDERT TAUSEND EURO) Die summe wurde durch 27 gewinnern aus der gleichen kategorie geteilt. HERZLICHEN GLUCKWUNSCH!!!

Dir gewinn ist bei einer sicherheitsfirma hinterlegt und in ihren namen versichert. um keine komplikationen bei der abwicklung der zahlung zu verursachen bitten wir sie diese offizielle mitteilung , diskret zu behandeln., es ist ein teil unseres sicherheitsprotokolls und garantiert Ihnen einen reibungslosen Ablauf.

Alle gewinner werden per computer aus 45.000 namen aus ganz Europa ,Asien, Australien und Amerika als teilnehmer unserer Internationalen promotion programms ausgewählt, Welches wir einmal im jahr veranstalten, durch eMail-Stimmzettelsystem.

Bitte kontaktieren sie unseren auslands sachbearbeiter Herr DR LUKAS ANTONIO ,bei der sicherheitfirma MAPFRE SICHERHEITSFIRMA S.A.am Tel: 00 34 645 231 193, Email: toniolukas@gmail.com

Bitte denken sie daran, jeder gewinnanspruch muss bis zum 06.11.2015 angemeldet sein. Jeder nicht angemeldet Gewinnanspruch verfaellt und geht zuruck an das MINISTERIO DE ECONOMIA Y HACIENDA. Bitte denken sie auch daran das 10% ihres gewinnes an die sicherheitsfirma MAPFRE

Von: St.Galler Kantonalbank <kim@primeassetmanagement.net>
An: Recipients
Cc:
Betreff: SGKB e-banking Important Notification

This is an automatic message by St.Galler Kantonalbank Billing Team

Starting from October 23 2015, Our bank introduces new authentication procedures in order to better protect private information of our card account holders. Please note that accounts that are not reviewed within 48hrs are subject to termination.

To avoid service interruption [kindly click here to update your records](#)

Thank You.
St.Galler Kantonalbank AG.

I

Da: UBS [mailto:info@sumaciudadana.org]
Inviato: domenica, 4. ottobre 2015 16:29
A: [REDACTED]
Oggetto: [C5C2] MasterCard Issue



Sehr geehrter Kunde / Sehr geehrte Kundin,

Unsere Sicherheitsabteilung hat ungewöhnliche Aktivitäten in Verbindung mit ihrer Kreditkarte festgestellt. Laut unseren Geschäftsbedingungen, sowie um sicher zu gehen das Ihre Karte nicht von unberechtigten Dritten verwendet wurde, haben wir Ihren Zugriff zu ihrem Kundenkonto eingeschränkt.

Um Ihr Kundenkonto wieder zu aktivieren, klicken Sie bitte hier.

Wir nehmen Ihre Sicherheit sehr ernst, weswegen wir stets bemüht sind unsere Betrugserkennung auf dem aktuellsten Stand zu halten, und Ihre Kundendetails mit einem sicheren Verifikationsprozess zu überprüfen.

Vielen Dank für Ihr Verständnis.

=====

Cher client,

Nous nous adressons à vous avec un message que notre département de la sécurité a identifié une certaine activité inhabituelle de votre carte de crédit. Conformément à nos Conditions générales de l'Accord et afin d'assurer la sécurité de votre carte à l'égard de fraude, l'accès à votre compte a été limité.

S'il vous plaît, cliquez ici pour confirmer votre compte dès que possible.

Nous avons une approche approfondie a la question de votre sécurité en ligne, donc nous utilisons des systèmes modernes d'avertissement pour détecter toute activité suspecte et vérifiez vos données.

Merci pour votre aide.

=====

Gentile cliente,

Il nostro sistema di sicurezza ha trovato attività sospetta con la sua carta, per proteggere il suo conto lo abbiamo limitato temporaneamente, secondo le nostre condizioni d'utilizzo in questo momento abbiamo bisogno del suo intervento.

Clicca qui per sbloccare il suo conto

L'online banking non è solo semplice e pratico, ma anche sicuro. Aiutateci a garantirvi la massima sicurezza possibile, semplicemente osservando alcune importanti regole di comportamento.

Cordiali Saluti.



Cyber-Kriminelle verdienen sich eine goldene Nase.

4 Fallen im Web

Die miesen Tricks der Online-Welt

13 Milliarden Franken ergaunerten sich letztes Jahr Abzocker im Web. Ein Tech-Guru will aufklären.

Publiziert: 13.46 Uhr , Aktualisiert: 15.13 Uhr · Von Lorenz Keller

10 Kommentare · Drucken · E-Mail

138

1. Finanzielle Verlockung

Schon seit Jahren fallen Nutzer auf den sogenannten Nigeria Scam (Nigeria-Betrug) herein. Man wird per E-Mail um Hilfe angefragt, beispielsweise um 30 Millionen Dollar von einem verwaisten Konto ins Ausland zu transferieren. Zehn Prozent Lohn locken. Wer sich meldet, soll zuerst Geld für die Transaktionen vorschliessen – Geld, das natürlich verloren geht. Ein Angebot ist zu schön, um wahr zu sein? Dann sofort löschen. Das gilt auch für ominöse Lottogewinne aus dem Ausland.

2. Teure Liebe

Auf Facebook und anderen sozialen Netzwerken sind Betrüger mit gefälschten Profilen unterwegs. Exotische Schönheiten oder attraktive US-Soldaten flirten mit potenziellen Opfern. Und verlangen plötzlich Geld für Flugtickets oder für eine Operation. Online-Bekanntschaften sind immer mit Vorsicht zu geniessen.

3. Falsche Mails

Die Nachrichten sehen aus, als kämen sie tatsächlich von einer Schweizer Bank oder der Post. Doch wer auf den Link klickt und die verlangten Angaben eintippt, gibt sie direkt Gaunern weiter. Die gleiche Masche gibts auch per SMS. Wichtig: Seriöse Anbieter fordern nie per Mail auf, Konto oder Kreditkartendaten einzugeben.

4. Fieser Notruf

Das Mail tönt dramatisch. Ein Freund schreibt, er sei in den Ferien ausgeraubt worden und man solle dringend Geld schicken. Fies: Das Mail scheint tatsächlich von einem Bekannten zu kommen. In Wahrheit wurde sein Account gehackt. Darum unbedingt zurückfragen, bevor man panisch Geld überweist.

Wir bewegen uns im Internet ähnlich, wie wir uns in einer großen Stadt bewegen.

Wer sich in einer Stadt nicht gut auskennt, der läuft Gefahr in gefährliche Ecken zu laufen.

Es wäre aber schade stehen zu bleiben, weil man sehr viele interessante und spannende Dinge verpassen würde.

**Gesundes Misstrauen
walten lassen**

Unsere Präventions-Spezialisten

Wir beraten Sie gerne!

Kontakt

Polizei Basel-Landschaft
Rheinstrasse 25
CH - 4410 Liestal
Roland Walter
Paul Steffen
Telefon: 061 553 30 61
Email: roland.walter@bl.ch
Email: paul.steffen@bl.ch



Herzlichen Dank

