

verbraucherzentrale

Sachsen

CYBER CRIME – VERBRAUCHER ALS OPFER? SELBSTSCHUTZ IST MÖGLICH

Dr. Katja Henschler, Verbraucherzentrale Sachsen

SPAM UND PHISHING (E-MAIL)

Amazon.de-Konto Überprüfen

Von Amazon +

An

amazon.de

Guten Tag,

Um Ihr Amazon-Konto vollständig zu aktivieren, verifizieren Sie dieses bitte. Die Verifizierung ist ganz einfach und erfordert nur wenige Schritte.

Klicken Sie auf den nachstehenden Link:

[Kontoinformationen aktualisieren](#)

Bitte antworten Sie nicht auf diese E-Mail. Dieses Postfach wird nicht überwacht, deshalb werden Sie keine Antwort erhalten.

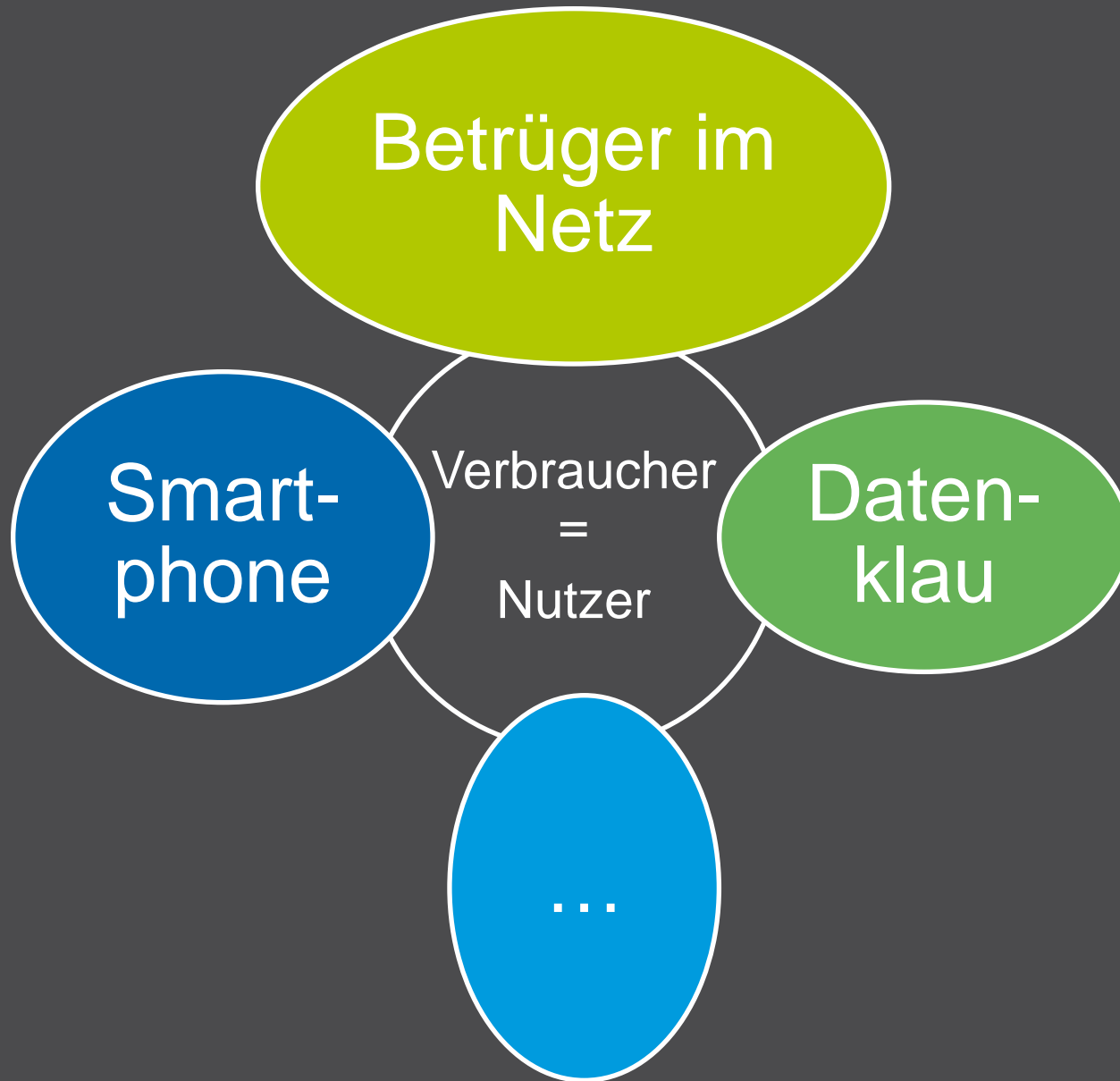
© 1998-2013, Amazon.com, Inc. oder Tochtergesellschaften

vbpx57ng.zone302.com/jgp/?c2fyX2hpc3MxOHhaG9vLnRl

SPAM UND PHISHING (E-MAIL)

EINORDNUNG

- **STÄNDIGE ZUNAHME**
- **TÄGLICHE MELDUNGEN / BESCHWERDEN VON VERBRAUCHERN**
- **IMMER RAFFINIERTER:**
 - täuschend echt, extrem hohe Verwechslungsgefahr,
 - besonders z.B. bei scheinbarem Absender Amazon und Paypal
 - persönliche Anrede des Empfängers



SPAM UND PHISHING (E-MAIL)

WAS WIR RATEN

- **Generell höchste Vorsicht und Skepsis bei allen Mails, die nicht von Bekannten und Vertrauten kommen!**
- Seriöse Anbieter melden sich grundsätzlich nicht per Mail
- Seriöse Rechnungen kommen in engem zeitlichen Zusammenhang mit Bestellung



VORSICHT
SPAM

SPAM UND PHISHING (E-MAIL)

WAS WIR RATEN

- Achtung wütende Bürger: Spam-Mails niemals antworten
- Öffnen der Mail selbst idR kein Problem, aber niemals die Anhänge oder Links
- Auf Internetseite des scheinbaren Anbieters nach Hinweisen suchen
- Betrugsverdacht dort auch melden



SPAM UND PHISHING (E-MAIL)

WAS WIR RATEN

- **Anzeige bei der Polizei – zumindest bei Verdacht**
- **Stets aktueller Virenschutz auf PC / Laptop und mobilen Endgeräten!**



SPAM UND PHISHING (E-MAIL)

BETROFFENHEIT DER VERBRAUCHER

- **Virus auf dem PC**
- **Insb. nach Antwort auf Spam-Mail:**
 - **noch mehr Spam**
 - **Datendiebstahl (mit der Folge der Gefahr von Identitätsdiebstahl)**
- **Geleistete Zahlungen auf gefakte Rechnungen**
- **Gefühl, nicht mehr vertrauen zu können**



BETRUG VIA SMARTPHONE

EINORDNUNG

- Nutzer finden plötzlich Forderung eines Drittanbieters auf Mobilfunkrechnung
- Grund der Forderung meist unklar
 - Werbe-Link in SMS / Whatsapp o.ä. geklickt
 - Werbefeld beim Surfen geklickt
 - ???



BETRUG VIA SMARTPHONE

EINORDNUNG

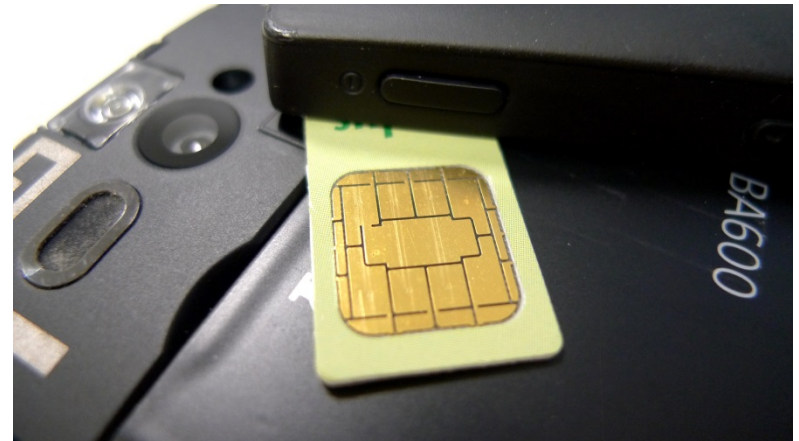
- Mobilfunkanbieter und Drittanbieter arbeiten Hand in Hand
- Verdacht gezielter „Abzocke“



BETRUG VIA SMARTPHONE

WAS RATEN WIR?

- **Forderung widersprechen**
- **Keinesfalls zahlen**
- **Drittanbietersperre ! ! !**
- **Ggf. Anzeige bei der Polizei**



BETRUG VIA SMARTPHONE



WERBEANRUF UND CALL-ID-SPOOFING

EINORDNUNG

- Anrufe unter einer für den Angerufenen vorgetäuschten Nummer: bei der Rufnummernanzeige des angerufenen Telefons wird anstatt der Originalrufnummer des Anrufers eine in der Regel frei wählbare Nummer (oder theoretisch auch ein Wort) angezeigt
- Anrufe erfolgen mit dem Ziel, Angerufenen zu betrügen: v.a. Geltendmachung tatsächlich nicht existierender Forderungen



WERBEANRUF UND CALL-ID-SPOOFING

WAS WIR RATEN

- Bei Anrufen Unbekannter gleich auflegen, gar nicht auf ein Gespräch einlassen (besonders Ältere sind den geschulten Telefonverkäufern nicht gewachsen)



WERBEANRUF UND CALL-ID-SPOOFING

WAS WIR RATEN

- Bundesnetzagentur informieren (BNA kann Nummern abschalten lassen; als Behörde aber sehr schwerfällig)
- Sensibler Umgang mit eigenen Daten – keine unbedachte Angabe eigener Telefonnummer!
- Bei Vortäuschung anderer Identität des Anrufers unbedingt Anzeige bei der Polizei



WERBEANRUF UND CALL-ID-SPOOFING

BETROFFENHEIT DER VERBRAUCHER

- Öfters erfolgreicher Betrug: Fälle hoher Geldzahlungen durch Betroffene auf Anrufe hin
- Betroffene sind von Werbeanrufen per se ungeheuer genervt
- Angst vorm Telefonklingeln
- Gefühl des Eindringens in häuslichen Bereich
- Genereller Vertrauensverlust
- Hilflosigkeit



IDENTITÄSKLAU

EINORDNUNG

- Ein Dritter nutzt meine (Online-)Identität:
 - E-Mail-Adresse
 - Amazon-Konto
 - Paypal-Konto
 - Facebook-Konto u.v.m.
- Kauft auf meine Kosten ein
- Gibt sich u.U. auch anderweitig als meine Person aus (Facebook-Einträge)

„?
Wer
bin ich
– und, wenn ja,
Wieviele
?“

IDENTITÄSKLAU

WAS RATEN WIR GENERELL BEI DATENMISSBRAUCH?

- Zwingend Anzeige bei der Polizei
- Neue – jeweils unterschiedliche - Passwörter für alle Online-Konten
- Bankkonten regelmäßig kontrollieren

„?
Wer
bin ich
- und, wenn ja,
Wieviele
?“

IDENTITÄSKLAU

BETROFFENHEIT DER VERBRAUCHER

- Potentiell oder real hohe finanzielle Schäden
- Große Schwierigkeiten beim Nachweis des Missbrauchs („Von Ihrer Mail-Adresse aus wurde doch bestellt!“)
- Angst
- Gefühl des Eindringens in intimste Sphären
- Genereller Vertrauensverlust

„?
Wer
bin ich
- und, wenn ja,
Wieviele
?“

LOVE-SCAMMING

EINORDNUNG

- Heiratsschwindel im Internet / in sozialen Netzwerken / auf Partnersuch-Portalen
- Gestohlene Profilbilder
- Scammer legen sich Legende mit ungewöhnlicher Lebensgeschichte zu, sind oft auf Mitleid aus, vermitteln seriösen Eindruck



LOVE-SCAMMING

EINORDNUNG

- Längere intensive regelmäßige Kontakte, auch telefonisch
- Nach gewisser Dauer zB vorgebliche Auslandsreise nötig; dann Schwierigkeiten zB mit Flugticket oder Visum und dringender kurzfristiger Geldbedarf vorgespielt; Übergabe per Western Union erbeten gepaart mit dauernden Liebesbeteuerungen
- vertrauensseliges Opfer zahlt



LOVE-SCAMMING

WAS RATEN WIR

- Präventiv: Aufklärung
- Repressiv: Anzeige bei der Polizei

Über uns | Newsletter | Links | Kontakt | Impressum | Suche

Polizeiliche Kriminalprävention der Länder und des Bundes

Suche nach Themen, Tipps, Hilfestellungen ... Absenden

Wir wollen, dass Sie sicher leben. Ihre Polizei. Kompetent. Kostenlos. Neutral.

Startseite und Aktionen | Themen und Tipps | Opferinformationen | Medienangebot | Presse

Sie sind hier: [Themen und Tipps](#) / [Betrug](#) / [Scamming](#) / [Romance-Scamming](#)

Betrug

- Haustürbetrug
- Kredit- und Anlagebetrug
- Falschgeld
- EC- und Kreditkartenbetrug
- Betrug an Geldautomaten
- Arzneimittel
- Scamming
 - Romance-Scamming
 - Rat und Hilfe
 - Folgen
- Finanzagenten
- Einzeltrick
- Timesharing
- Unerlaubte Werbeanrufe
- Geldwäsche
- Gewinnversprechen

Diebstahl und Einbruch

- Drogen
- Gefahren im Internet
- Gewalt
- Jugendkriminalität

Romance- oder Love-Scamming

Ein kurzer Chat oder eine nette Mail von einem Unbekannten – das so genannte **Love- oder Romance-Scamming** fängt harmlos an.

Die Scammer suchen **auf Online-Partnerbörsen oder in sozialen Netzwerken** wie Myspace oder Facebook nach Opfern, sie gehen Mitgliederlisten durch oder verwenden Adressen aus Yahoo oder dem MSN-Messenger. Eine kurze Online-Einladung zum Chat dient vielen als Erstkontakt. Um sich beim potenziellen Opfer interessant zu machen, legen sich die Scammer **ungewöhnliche Lebensgeschichten** zu – und sie hinterlassen immer einen seriösen Eindruck.

Typische Scammer-Profile

Scamm-Männer geben sich als Ingenieure, Architekten, Soziologen, Konstrukteure in der Ölindustrie oder als Tierärzte und Computerspezialisten aus. Auf den Fotos des Scammer-Profiles bekommen weibliche Opfer eine attraktive weiße Person präsentiert – **die Bilder sind allerdings gestohlen**. Und auch wenn der "Neue" vorgibt, in Amerika oder im europäischen Ausland zu leben, so sitzt er wahrscheinlich in Westafrika. Davon merken die Opfer allerdings nichts, denn diese Chat-Bekanntschäften sprechen perfekt Englisch oder benutzen kostspielige Übersetzungstools für ihre Mails.

Medien zum Thema

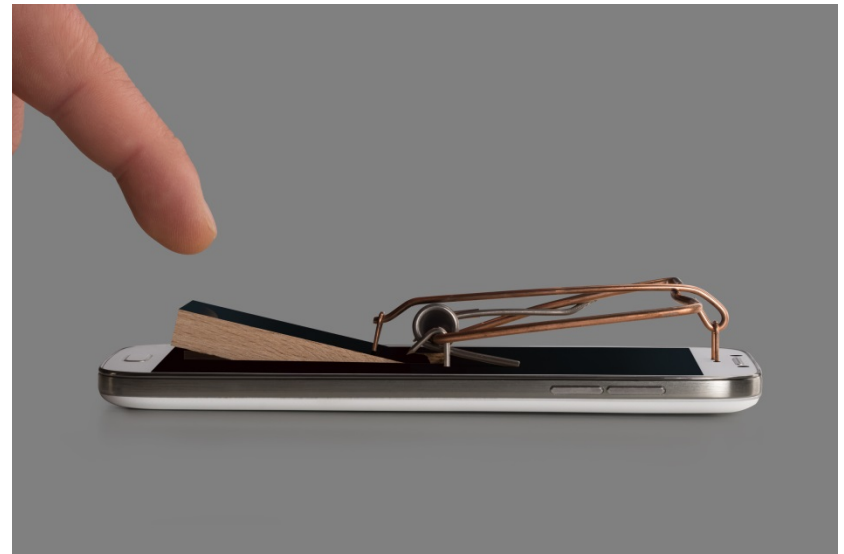
INFORMATIONSDIENST

Vorauszahlungsbetrug / betrügerische Angebote im Internet, überzahlte Schecks, 'Nigeria-Briefe'

LOVE-SCAMMING

BETROFFENHEIT DER VERBRAUCHER

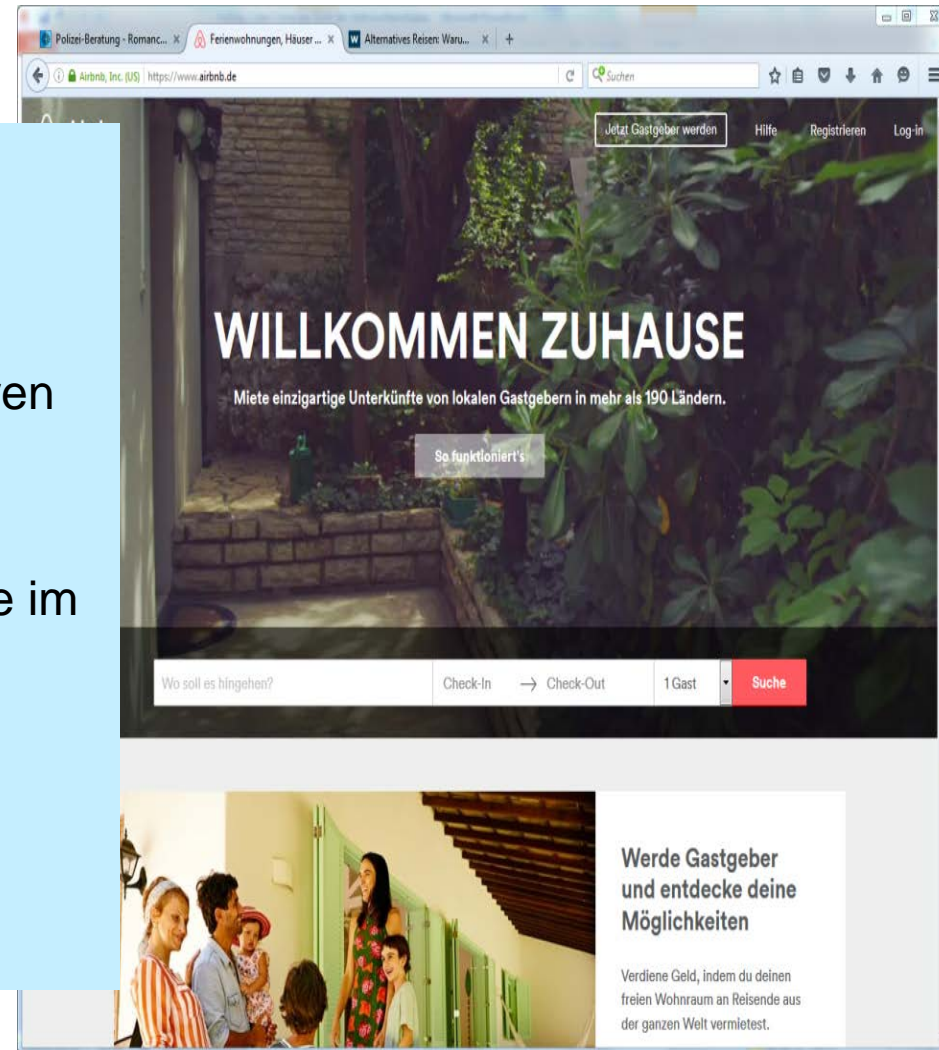
- Finanzielle Schäden
- Angst
- Zunehmende Verunsicherung



BETRUG AUF ANZEIGEN-PORTALEN

EINORDNUNG

- Z.B. airbnb.de
- Private lokale Gastgeber präsentieren Unterkünfte (hochwertige Fotos, günstige Preise)
- Sitzen selbst oft (vorgeblich) gerade im Ausland
- Vorkassezahlung an ausländisches Konto



BETRUG AUF ANZEIGEN-PORTALEN

WAS RATEN WIR

- Präventiv: Aufklärung
- Repressiv: Anzeige bei der Polizei



BETRUG BEI FAKE-SHOPS

EINORDNUNG

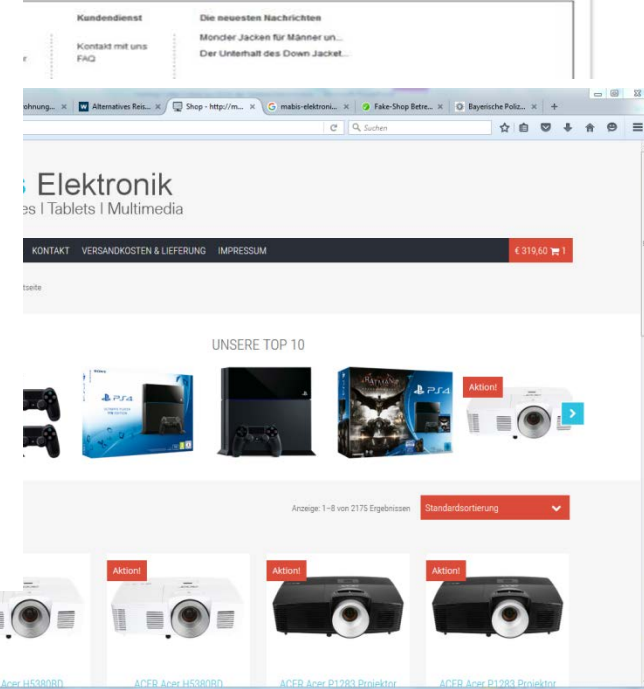
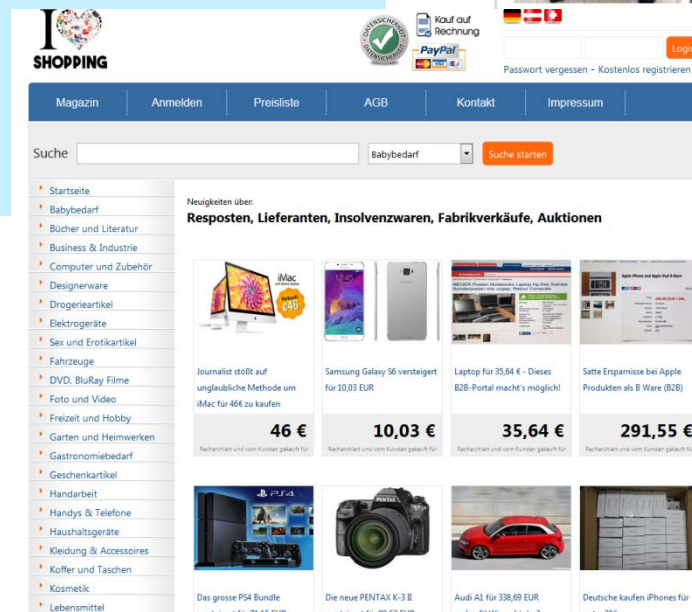
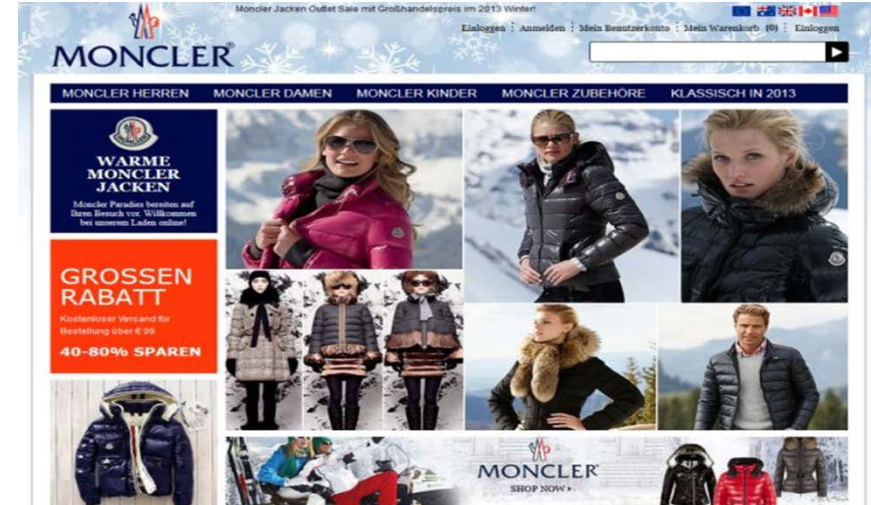
- Meist keine Lieferung bestellter Ware
- Seiten werben mit z.T. unrealistisch günstigen Preisen
- v.a. Elektronikartikel betroffen
- Seitenbetreiber (Impressum) meist nicht im Handelsregister eingetragen
- i.d.R Vorkasse, Paypal ausgeschlossen
- Konto des Empfängers meist im Ausland
- z.T. kein Impressum oder / und AGB
- Bekannte Logos geben Anschein der Seriösität



BETRUG BEI FAKE-SHOPS

WAS RATEN WIR

- Vor Bestellung bei unbekanntenen Anbietern unbedingt nach Erfahrungen im Netz suchen
- Möglichst nie Vorkasse-Zahlungen, höchstens bei vertrauten Anbietern
- Anzeige bei der Polizei erstatten



BETRUG AUF FAKE-SHOPS

BETROFFENHEIT DER VERBRAUCHER

- Finanzielle Schäden
- Ärger

ABOFALLEN

The screenshot shows a web browser window with several tabs open. The active tab is 'maps-routenpl...'. The address bar shows 'maps-routenplaner.info'. The main content area features a route calculation form with the following details:

Startadresse		Zieladresse	
Sonnenschein	8	Panoramastraße	1
48565 Steinfurt		10178 Berlin	
Deutschland		Deutschland	

Additional options include 'Autobahn vermeiden', 'Mit dem Auto', and 'Fußweg'. A 'Route berechnen' button is present.

Below the form is a promotional banner for a 'KOSTENLOSES GEWINNSPIEL:'. It includes a link: [-> HIER <- klicken um zum Gewinnspiel zu gelangen](#). The text reads: 'Unter allen Usern verlosen wir ein neues' followed by an image of a TomTom navigation device showing a route to 'Berlin-Zentrum'. Below the image, it says 'sowie eine Reise für 2 Personen auf die Malediven' and another link: [-> HIER <- klicken um zum Gewinnspiel zu gelangen](#).

The right sidebar contains a 'Hauptmenü' with 'Startseite', a 'Memberbereich' with fields for 'Benutzername' and 'Passwort', and an 'Anmelden' button. Below this are links for 'Passwort vergessen?' and 'Neutransfer'. Further down is a 'Userinfos' section with links for 'Gewinnspiel', 'Datenschutz', 'Widerrufsrecht', 'Nutzungsbedingungen', and 'Impressum'. At the bottom is a 'Hinweis' section with a disclaimer: 'Geben Sie einfach in das linke Eingabefeld ihre Startadresse und im rechten Eingabefeld ihre Zieladresse ein und Sie erhalten eine detaillierte Beschreibung wie Sie an ihr Ziel kommen. (Wannville können Sie auch eingeben, ob Sie mit dem Auto oder zu Fuß unterwegs sind. Wir wünschen Ihnen viel Vergnügen mit unserem Service. Die 24 Monate Mitgliedschaft kostet bei Anmeldung 500,- Euro, die Abrechnung erfolgt im Voraus. Bitte beachten Sie, dass Sie bei Missbrauch unseres Services mit Straf- und Zurechenlichen Folgen rechnen müssen.'

The browser's address bar at the bottom shows the URL: 'maps-routenplaner.info/component/users/?view=registration'.

ABOFALLEN

EINORDUNG

- Nutzer suchen eine typischerweise kostenfreie Dienstleistung im Netz, z.B. Routenplaner
- Tragen – gedankenlos – ihre persönlichen Daten in die Maske ein
- Übersehen „Hinweis“ am Rand, dass dadurch Abschluss kostenpflichtiger Mitgliedschaft über z.B. 500 Euro

Hinweis

Geben Sie einfach in das linke Eingabefeld Ihre Startadresse und im rechten Eingabefeld Ihre Zieladresse ein und Sie erhalten eine detaillierte Beschreibung wie Sie an Ihr Ziel kommen. Wahlweise können Sie auch eingeben, ob Sie mit dem Auto oder zu Fuß unterwegs sind. Wir wünschen Ihnen viel Vergnügen mit unserem Service. Die 24 Monate Mitgliedschaft kostet bei Anmeldung 500,- Euro, die Abrechnung erfolgt im Voraus. Bitte beachten Sie, dass Sie bei Missbrauch unseres Services mit Straf- und Zivilrechtlichen Folgen rechnen müssen.

ABOFALLEN

WAS RATEN WIR

- Vertrag anfechten
- Widerruf erklären
- Keinesfalls zahlen!!!
- Immer Vorsicht, wenn Eingabe persönlicher Daten bei (vermeintlich) kostenfreier Dienstleistung erfragt wird

WIEDER DA:
ABOFALLEN
IM NETZ



ABOFALLEN

BETROFFENHEIT DER VERBRAUCHER

- Masche der Anbieter: großer Druck auf Nutzer, endlich zu zahlen, durch Drohung mit Inkasso, noch höheren Kosten für Mahnungen, Gerichtsvollzieher etc.
- dadurch „Mürbemachen“ der Nutzer, weil viele die Drohungen und die gesamte Belastung nicht aushalten



SCHLÜSSELDIENSTE

WAS RATEN WIR

- Masche der Anbieter: großer Druck auf Nutzer, endlich zu zahlen, durch Drohung mit Inkasso, noch höheren Kosten für Mahnungen, Gerichtsvollzieher etc.
- dadurch „Müribemachen“ der Nutzer, weil viele die Drohungen und die gesamte Belastung nicht aushalten

The screenshot shows a web browser displaying the website of the Verbraucherzentrale Sachsen. The page features a navigation menu with options like 'Beratung', 'Veranstaltungen', 'Presse', and 'Wir über uns'. A prominent yellow banner displays a family photo. Below this, a search bar and a breadcrumb trail 'Presse → Pressearchiv → 2015 → Inkasso aus dem Ausland' are visible. The main content area contains a news article dated 03.08.2015 titled 'Inkasso aus dem Ausland' with the sub-headline 'Nicht zahlen, sondern Inkasso-Abzocker stellen'. The article text discusses a legal case involving a lottery operator and a law firm, warning consumers not to pay. A sidebar on the right includes a search bar and a section 'Sie finden uns auch auf' with a Facebook link to 'www.facebook.com/VZSachsen'. The footer of the page contains the URL 'www.verbraucherzentrale-sachsen.de/Willkommen-im-Pressportal-1'.

10 Regeln für sicheres Surfen im Netz

Sicherheitskompass

von: Polizeiliche Kriminalprävention der Länder und des Bundes
+ Bundesamts für Sicherheit in der Informationstechnik (BSI)



<http://www.polizei-beratung.de/themen-und-tipps/gefahren-im-internet/sicherheitskompass.html>

10 REGELN FÜR SICHERES SURFEN IM NETZ SICHERHEITSKOMPASS

1. HARDWARESCHUTZ
2. WLAN SICHERN
3. RECHTE EINSCHRÄNKEN
4. SOFTWARE UPDATEN
5. VIRENSCANNER & FIREWALL
6. BROWSERSICHERHEIT
7. E-MAILS
8. VORSICHT VOR INTERNETDOWNLOAD
9. DATENSPARSAMKEIT
10. SICHERES PASSWORT

Regel 1: Hardwareerschutz

- Schutz gegen Diebstahl/unbefugten Zugriff
- Tastatursperre und Passwort-/Pinabfrage

Regel 2: WLAN sichern

- Aktivierung der WLAN-Funktion nur bei Bedarf
- gesicherte Verbindung (Schloss-Symbol)

Regel 3: Rechte einschränken

- eigenes Benutzerkonto für jeden Benutzer
- nicht mit Administratorenrechten im Internet surfen

Regel 4: Software updaten

- Alle verfügbaren Updates zeitnah installieren
- automatische Updates

Regel 5: Virens Scanner & Firewall

- Firewall aktivieren, über Sicherheitscenter Betriebssystem
- kostenfreies Antiviren-Schutzprogramm

Regel 6: Browsersicherheit

- Wahl der höchsten Sicherheitsstufe
- Warnungen vor infizierten Seiten etc. einstellen

Regel 7: E-Mails

- Anhänge und Links nur bei bekannten Absendern öffnen

Regel 8: Vorsicht vor Internetdownload

- Software möglichst von Herstellerseite downloaden
- Prüfung durch Antivirenprogramm

Regel 9: Datensparsamkeit

- Zurückhaltung bei Angabe persönlicher Daten
- Auf Verschlüsselung achten (<https://>)

Regel 10: sicheres Passwort

- Groß- und Kleinbuchstaben, Zahlen, Sonderzeichen
- keine Namen bzw. gängigen Wiederholungs-/Tastaturmuster (abc, 123aa, asdfgh)
- Beispiele für sichere Passwörter, die sich gut merken lassen: Satz bilden

MsiaupmZ!

„Morgens stehe ich auf und putze meine Zähne!“

Aj1.&3.SiMsiH!

„An jedem 1. und 3. Samstag im Monat spiele ich Handball!“

VIELEN DANK FÜR IHRE AUFMERKSAMKEIT

verbraucherzentrale

Sachsen

Impressum

Verbraucherzentrale
Sachsen e.V.

Katharinenstraße 17
04109 Leipzig

vzs@vzs.de

www.verbraucherzentrale-sachsen.de