



**Aufgeflogen:**  
Mazedonischer  
Bauarbeiter und  
Arbeitsmarkt-  
kontrolleur

## FILM

## 70-Stunden-Woche für 550 Franken pro Monat

Ulrich Grossenbacher zeigt, wie in der Schweiz ausländische Schwarzarbeiter ausgenutzt werden.

Arbeitsmarktkontrolleure sind nirgends willkommen. Sie tauchen unangemeldet an Orten auf, an denen sie Verstösse gegen das Arbeitsrecht vermuten. Oft werden sie fündig, wie der Dokumentarfilm «Schwarzarbeit» von Regisseur Ulrich Grossenbacher zeigt. Er begleitete fünf Kontrolleure 70 Tage lang bei ihrer Arbeit.

Auf ihren Kontrolltouren stossen die Inspektoren auf zum Teil krasse Verletzungen des Arbeitsrechts. Etwa in einem Lebens-

mittelladen, in dem der Manager an sieben Tagen pro Woche je zehn Stunden arbeitet und dafür einen Grundlohn von 550 Franken erhält. Oder in einem Privathaushalt, in dem eine Pflegerin einen Patienten sieben Tage pro Woche rund um die Uhr betreuen muss, obwohl im Vertrag nur sechseinhalb Stunden pro Tag stehen. Der Lohn wurde ihr mündlich versprochen - bis jetzt hat sie noch keinen Rappen davon gesehen.

Die Arbeit der Kontrolleure ist frustrierend. Denn oft kommen die Arbeitgeber mit einer Busse davon. Anders sieht es für die aufgefliegenen Schwarzarbeiter aus, häufig Asylbewerber oder illegal Eingewanderte.

Sie werden von der Polizei abgeholt und im schlimmsten Fall ausgeschafft. Die Kontrolleure gehen unterschiedlich mit ihrer Verantwortung um. Der eine würde die Schwarzarbeiter am liebsten laufen lassen, der andere möglichst alle verhaften und ausschaffen lassen. «Schwarzarbeit» ist ein bewegender Film. Er ist dank zum Teil amüsanten Dialogen zwischen den Kontrolleuren aber auch unterhaltsam. Der Film läuft ab dem 28. April in Deutschschweizer Kinos. *Marc Mair-Noack*

«Schwarzarbeit», Ulrich Grossenbacher, 109 Minuten, Fair & Ugly 2021

## BUCH

## Medien bewusster konsumieren

Nachrichten in den Medien sind selten Stimmungsaufheller. Das gilt nicht nur in Kriegszeiten. Sie beeinflussen, wie man abstimmt und wählt, was man kauft - und sie können sogar die Gesundheit gefährden. Ob Terror, Krieg oder Pandemie: Je mehr über Katastrophen berichtet wird, desto grösser wird die Angst, selbst in Gefahr zu sein.

Wie entkommt man dieser Negativspirale und bleibt trotzdem gut informiert? Und welche Chancen böte ein Journalismus, der den Finger nicht nur auf wunde Punkte legt, sondern auch aufzeigt, wie sich Dinge zum Besseren wenden?

Diesen Fragen geht die deutsche Autorin Ronja von Wurmb-Seibel in ihrem neuen Buch «Wie

wir die Welt sehen» nach. Die 36-Jährige ist kein naiver Schöngeist. Sie arbeitete als Reporterin im kriegsversehrten Afghanistan, schrieb Beiträge über traumatisierte Bundeswehrsoldaten und Kinderarmut. Ein erhellendes Buch, das die Mechanismen des Journalismus erklärt und aufzeigt, wie man Medien bewusster konsumieren kann. *leu*



Ronja von Wurmb-Seibel, «Wie wir die Welt sehen», Kösel-Verlag, München 2022, rund 240 Seiten, ca. 30 Franken

# So schützt man sich vor Internetbetrüchern

**Gefälschte E-Mails, manipulierte Dokumente, unsichere Programme: Mit zahlreichen Tricks versuchen Betrüger, Zugriff auf fremde Computer und Handys zu bekommen. saldo zeigt, wie man solche Angriffe abwehrt.**

Constanze Lullies aus Küsnacht ZH betrieb eine eigene Website beim Internetprovider Hostpoint. Im Januar erhielt sie mehrere E-Mails - angeblich von Hostpoint-Mitarbeitern in Rapperswil-Jona SG. Alle hatten denselben Inhalt: Ihr Abo laufe ab. Wenn sie nicht umgehend zahle, sei ihre Website bald nicht mehr online.

Lullies klickte in der E-Mail-Nachricht auf einen Link und gab ihre Kreditkartendaten ein, um das Abo zu erneuern. Es erschien die Meldung, die Transaktion habe nicht funktioniert. Was die Kundin nicht wusste: Die E-Mails waren gefälscht. Die Karteninformationen landeten direkt bei den Betrügern. Abends entdeckte Constanze Lullies, dass 1200 Euro von ihrer Kreditkarte der Post-

finance abgebucht waren. Sie liess die Karte sofort sperren. Doch das Geld war weg. Postfinance stellte sich quer und behauptete, die Kundin habe die Transaktion auf dem Handy bestätigt.

Solche gefälschten E-Mails - sogenannte Phishingmails - sind verbreitet. Die Empfänger werden verleitet, auf einen Link zu klicken, der sie auf eine betrügerische Website führt. Dort sollen sie ihre Kreditkarteninfos eingeben. Viele dieser E-Mails stammen aus vermeintlich unverdächtigen Quellen - etwa von der Post. In den letzten Wochen erhielten *saldo*-Leser Phishingmails mit dem Absender des Eidgenössischen Finanzdepartementes, Abteilung Zoll. Darin wurde eine Zollgebühr für ein angebliches Paket aus dem Ausland verlangt.

## Das sollten Opfer von Betrügern sofort tun

- Falls die Betrüger Kreditkartendaten kennen, sollte man die Karte umgehend sperren. Wurde bereits Geld abgeboben, den Betrag per Einschreiben sofort bei der Kreditkartenfirma beanstanden und Anzeige erstatten.
- Den Computer kann man mit einem Virens scanner über-

prüfen. Hat man keinen Zugang mehr zum Mailkonto, auf «Passwort vergessen» klicken.

- Falls das nichts hilft, sollte man telefonisch beim Mailbox-Betreiber intervenieren und das Mail-Passwort sowie andere wichtige Passwörter ändern.



**Constanze Lullies:** Betrüger erschlichen sich ihre Kreditkartendaten

Neben Phishing arbeiten die Betrüger auch mit anderen Tricks. Zum Beispiel locken sie die Benutzer auf Internetseiten, von denen aus heimlich ein Programm heruntergeladen und auf dem Computer installiert wird. Diese Programme können den PC ausspionieren, Adressen und Passwörter stehlen oder die Daten auf dem Gerät verschlüsseln. Erst, wenn man die verlangte Summe bezahlt, erhält man den Zugang zu seinen Dateien zurück.

### Betrüger verstecken sich hinter bekannten Adressen

Das Risiko, auf Internetbetrüger hereinzufallen, lässt sich minimieren. Das sind die wichtigsten Tipps:

- Lassen Sie sich nie von einem angeblich dringenden E-Mail zeitlich unter Druck setzen.
- Misstrauen ist am Platz, wenn man in einem Mail auf einen Link klicken sollte. Im Zweifelsfall ist es sinnvoll, den Absender anzurufen und abzuklären, ob das E-Mail von ihm stammt.
- In mitgeschickten Dateien kann Software enthalten sein, die sich beim Öffnen auf dem Computer installiert. Besonders beliebt sind Office-Dateien wie Textdokumente oder Excel-Tabellen. Es kann nützlich sein, die Datei von der Website Virustotal.com scannen zu lassen: Einfach die Datei mit der Maus auf die Website ziehen und den Scan auf «Confirm upload» klicken. Nun wird die

## Frage & Antwort

Marc Mair-Noack  
Redaktor



Datei von über 50 Virensclannern geprüft.

- In Office-Dateien sollte man sogenannte Makros deaktivieren. Diese können Word- oder Excel-Aufgaben automatisch ausführen. Betrüger können die Makros auch für die Installation von Schadsoftware verwenden. Man kann die Makros von Microsoft-Office oder Libre-Office in den Einstellungen unter «Sicherheit» deaktivieren.

- Der im Posteingang angezeigte Absender eines E-Mails lässt sich leicht fälschen. Deshalb sollte man im Zweifelsfall auf den Absender klicken. Die meisten Mailprogramme zeigen daraufhin die Adresse an, von der die Nachricht tatsächlich kam. Bei Phishingmails unterscheidet sich die Adresse oft deutlich von jener des angeblichen Absenders. Verdächtig ist auch eine längere Zahlenkombination in der Mailadresse. Doch auch korrekte Adressen von Bekannten oder Familienangehörigen können von Betrügern missbraucht werden. Wurde das Mailkonto eines Benutzers gehackt, kann der Betrüger problemlos in seinem Namen E-Mails an sämtliche Personen im Adressbuch verschicken.

- Hacker suchen nach Sicherheitslücken in verbreiteten Programmen und Betriebssystemen. Auf diese Weise gelangen sie auf fremde Computer. Programmhersteller veröffentlichen deshalb regelmässig Updates, in denen Sicherheitslücken behoben werden sollen. Es lohnt sich, die Sicherheitsupdates aller Programme auszuführen.

- Für Windows-Anwender ist eine aktuelle Antivirensoftware Pflicht. Gut und sicher ist der in Windows eingebaute Defender. Mac-, iPhone- und Android-Benutzer brauchen

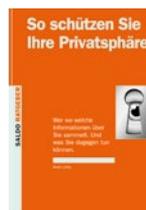
kein zusätzliches Antivirenprogramm.

- Ein Schadprogramm kann Daten löschen oder die ganze Festplatte verschlüsseln. Daher sollten die Daten regelmässig mit einem Sicherheits-Backup auf einer externen Festplatte gesichert werden. Wichtig: Die Festplatte sollte man nach dem Backup nicht am Computer eingesteckt lassen.

- Sichere Passwörter sind von Vorteil. Begriffe aus dem Wörterbuch sind unsicher. Besser sind Kombinationen aus Buchstaben, Sonderzeichen, Zahlen und schweizerdeutschen Begriffen. Tipp: Die Anfangsbuchstaben der Worte eines Satzes verwenden, den man sich gut merken kann.

Die Betrüger versuchen auch noch auf anderen Wegen, an den Computer oder persönliche Daten zu kommen. Zum Beispiel via Telefon: Angebliche Microsoft-Angestellte rufen an und behaupten, der PC sei infiziert. Sie versuchen, ihre Opfer dazu zu bringen, den PC einzuschalten und ihnen den Zugang darauf zu ermöglichen. Oder angebliche Bankangestellte wollen Zahlungsdaten erfahren. Solche Anrufe sind nicht seriös.

Marc Mair-Noack



Der *saldo*-Ratgeber **So schützen Sie Ihre Privatsphäre** (164 Seiten, Fr. 27.-) zeigt auf, welche privaten und staatlichen Stellen welche

Informationen sammeln. Und was man dagegen tun kann. Bestellen Sie das Buch mit dem Talon auf Seite 34 oder auf [www.saldo.ch](http://www.saldo.ch).

### Wie lassen sich Fotos automatisch öffnen?

«Wenn ich Fotos mit Firefox herunterlade, möchte ich, dass sie sich automatisch im Fotoprogramm öffnen. Wie geht das?»

Öffnen Sie die Firefox-Einstellungen und scrollen Sie bis zu «Dateien und Anwendungen». Dort sind einige Dateiformate aufgelistet. Rechts daneben steht, was beim Herunterladen einer solchen Datei passieren soll. Suchen Sie hier das gewünschte Fotodateiformat (wahrscheinlich jpeg). Rechts klicken Sie auf die eingestellte Aktion. Ist hier das gewünschte Fotoprogramm bereits aufgelistet, wählen Sie es aus. Ansonsten suchen Sie das Programm mit «Andere Anwendung». Sollte das Dateiformat noch nicht in den Einstellungen aufgelistet sein, müssen Sie zuvor irgendein Foto in diesem Format von einer Website herunterladen. Danach klicken Sie oben rechts im Firefox-Browser auf das Download-Symbol. Wählen Sie mit der rechten Maustaste die heruntergeladene Fotodatei und danach «Ähnliche Dateien immer öffnen». Nun können Sie in den Einstellungen wie oben beschrieben vorgehen.

### Wie passe ich den Finder auf dem Mac an?

«Auf meinem Mac sind im Finder links einige Ordner-Favoriten aufgelistet – etwa «Programme» oder «Dokumente». Kann ich auch einen eigenen Ordner hinzufügen?»

Ja. Bewegen Sie den gewünschten Ordner mit der Maus in die Seitenleiste des Finder-Ordners. Nun wird er dort aufgelistet. Das Entfernen geht ebenfalls mit der Maus.



Was wollten Sie zum Thema **Multimedia schon lange wissen?**

Schreiben Sie an: [redaktion@saldo.ch](mailto:redaktion@saldo.ch),  
Betreff «Multimedia-Fragen»