Cyberkriminalität

Nützliche Infos für Ihre persönliche Sicherheit

Bundesweites Opfer-Telefon 116 006
www.weisser-ring.de
www.facebook.com/WEISSERRING

WEISSER RING
Wir helfen Kriminalitätsopfern.

Herausgeber: WEISSER RING – Gemeinnütziger Verein zur Unterstützung von Kriminalitätsopfern und zur Verhütung von Straftaten e. V.

Bundesgeschäftsstelle: Weberstraße 16, 55130 Mainz 2/2017

Liebe Leserin, lieber Leser,

Sie halten gerade Ihr persönliches Exemplar „Nützliche Infos für Ihre persönliche Sicherheit“ in der Hand. Damit möchte der WEISSE RING Sie dabei unterstützen, sich wirksam vor kriminellen Gefahren zu schützen.

In dieser Ausgabe erfahren Sie einiges über Sicherheit in sozialen Netzwerken, wie Sie sich vor Daten-Klau und Phishing-Attacken schützen können und worauf Sie bei Internetaktivitäten generell achten sollten. Diese Infos sind mehrheitlich dem Internet-Portal polizei-beratung.de entnommen.

Vorbeugung ist der beste Opferschutz!
Diese Erkenntnis hat sich der WEISSE RING ebenso auf die Fahne geschrieben wie die schnelle, vielfältige und direkte Hilfe für die Menschen und ihre Angehörigen, die dennoch Opfer einer Straftat geworden sind.

Informationen über die Hilfsmöglichkeiten des WEISSEN RINGS geben wir Ihnen ebenfalls gerne mit auf den Weg.
Für Ihr Interesse an der Arbeit unseres gemeinnützigen Vereins sowie Ihre tatkräftige Unterstützung des Opferhilfegedankens, z. B. durch eine Spende oder die Mitgliedschaft im WEISSEN RING, sind wir Ihnen sehr dankbar.

Ein solches Zeichen humanitärer Verantwortung hilft Menschen in Not. Es verdient Respekt und Anerkennung.

In diesem Sinne wünschen wir Ihnen und Ihren Lieben
von Herzen alles Gute.

Ihr
WEISSER RING

Soziale Netzwerke sicher nutzen

Millionen Deutsche, darunter auch viele junge Menschen, knüpfen Kontakte und pflegen Freundschaften über das Internet. Doch wer in Facebook, Xing & Co. persönliche Informationen über Hobbys, die Familienverhältnisse oder den beruflichen Werdegang veröffentlichen will, sollte sich über die möglichen Gefahren bewusst sein.
Auf der Webseite www.bsi-fuer-buerger.de klärt das Bundesamt für Sicherheit in der Informationstechnik (BSI) über die Gefahren von sozialen Netzwerken auf.

Die zehn wichtigsten Tipps im Überblick:

1. Seien Sie zurückhaltend mit der Preisgabe persönlicher Informationen!
2. Erkundigen Sie sich über die Allgemeinen Geschäftsbedingungen und die Bestimmungen zum Datenschutz des genutzten sozialen Netzwerks!
3. Seien Sie wählerisch bei Kontaktanfragen – Kriminelle „sammeln" Freunde, um Personen zu schaden!
4. Melden Sie „Cyberstalker", die Sie unaufgefordert und dauerhaft über das soziale Netzwerk kontaktieren!
5. Verwenden Sie für jede Internetanwendung, insbesondere wenn Sie in verschiedenen sozialen Netzwerken angemeldet sind, ein unterschiedliches und sicheres Passwort!
6. Geben Sie keine vertraulichen Informationen über Ihren Arbeitgeber und Ihre Arbeit preis!
7. Prüfen Sie kritisch, welche Rechte Sie den Betreibern sozialer Netzwerke an den von Ihnen eingestellten Bildern, Texten und Informationen einräumen!
8. Wenn Sie „zweifelhafte" Anfragen von Bekannten erhalten, erkundigen Sie sich außerhalb sozialer Netzwerke nach der Vertrauenswürdigkeit dieser Nachricht!
9. Klicken Sie nicht wahllos auf Links – Soziale Netzwerke werden verstärkt dazu genutzt, um Phishing zu betreiben!
10. Sprechen Sie mit Ihren Kindern über deren Aktivitäten in sozialen Netzwerken. Klären Sie sie über die Gefahren auf!

Daten-Klauern rote Karte zeigen

Online-Banking boomt. Mittlerweile nutzt mehr als jeder zweite Internetnutzer auch die Möglichkeit zum virtuellen Bankbesuch. Die bequeme Art, Bankgeschäfte abzuwickeln, überzeugt viele Kunden. Rund um die Uhr – von Zuhause oder unterwegs.
Vor dem Hintergrund einer stetig steigenden Service-Nachfrage treffen die Kreditinstitute umfangreiche Sicherungsmaßnahmen, um ihre Internet-Kunden zu schützen. Diesen Schutz versuchen Kriminelle jedoch auszuhebeln. Ihre Masche: Sie versenden fingierte E-Mails, so genannte **Phishing-Mails**.

Der Trick: In betrügerischer Absicht werden Bankkunden mit täuschend echt aufgemachten E-Mails dazu veranlasst, über einen Link vermeintliche Internet-Seiten von Banken aufzurufen. Dort sollen dann persönliche Daten wie Zugangsdaten, Passwörter oder ähnliches eingegeben werden – angeblich aus Sicherheitsgründen, zur Bestätigung oder um, wie es oft heißt, Datenabgleiche auszuführen.

Tatsächlich landen die Kunden aber keinesfalls auf echten Bank-, sondern vielmehr auf gefälschten Internet-Seiten. Manchmal wird – als Variante dieser betrügerischen Tour – vor der eigentlichen Internet-Seite der Bank ein Pop-Up geöffnet, das zur Eingabe der Daten auffordert. Auch in diesen Fällen haben die Täter nur ein Ziel: Sensible Daten sollen abgefangen und für Betrügereien missbraucht werden. Der Empfänger soll dazu veranlasst werden, persönliche Daten wie Passwörter, Zugangsdaten, Transaktionsnummern usw. preiszugeben. Doch auch an weiteren persönlichen Daten wie Name, Geburtstag, Anschrift oder Bankverbindungen sind Daten-Klauer interessiert.

Die Methoden werden immer raffinierter. Kamen früher Mails in Umlauf, die – einfach gestrickt und schlecht formuliert – die Absicht des Absenders auf Anhieb verrieten, so ködern die Täter ihre Opfer heute mit professionell gestalteten Internet-Seiten, die selbst von Profis nur schwer als „Fake“ zu identifizieren sind.

Mit diesen persönlichen Daten können Betrüger Missbrauch betreiben (Identitätsdiebstahl = Übernahme einer fremden Identität) und mit der vorgegaukelten Identität online im Namen des Geschädigten nahezu alle Geschäfte abwickeln (Geld überweisen, Dispokredit ausschöpfen, Online-Einkäufe tätigen etc.). So entsteht Jahr für Jahr ein beträchtlicher wirtschaftlicher Schaden.

Was ist gegen Phishing-Attacken zu tun?

„Phishing“ ist prinzipiell nichts anderes als der landläufig bekannte Haustür-Betrug, der das Vertrauen und die Arglosigkeit von Menschen ausnutzt.

Deshalb: Informieren Sie sich besser einmal mehr als einmal zu wenig über den Absender der E-Mail. Sind Ihre persönlichen Daten erst einmal in der Hand der Täter, kann Ihnen hoher finanzieller Schaden entstehen.

Haben Sie den Verdacht, Opfer einer Phishing-Attacke geworden zu sein, heißt es schnell zu handeln.

- Sperren Sie sofort den Onlinezugang für das betroffene Konto bei Ihrem Kreditinstitut.
- Prüfen Sie, ob auf dem Konto Verfügungen vorgenommen wurden, die nicht von Ihnen stammen.
- Sichern Sie betrügerische Mails, die Sie erhalten haben.
- Erstatten Sie im Schadensfall Anzeige bei der Polizei.

Ärger haben auch die Unternehmen, in deren Namen die Betrüger auftreten. Denn sie erleiden oft einen Imageschaden. Prominentes Beispiel hierfür ist eBay. In der zur leichteren Bedienung des Portals verfügbaren Toolbar, einer Menüleiste unterhalb der Browser-Adressleiste, ist eine spezielle Sicherheitsfunktion integriert: Wenn man sich tatsächlich bei eBay befindet, leuchtet der Button „Sicherheits-Check“ grün. Andere Firmen arbeiten an ähnlichen Lösungen, um ihre Kunden zu schützen.

Auch die Banken greifen zu Gegenmaßnahmen. So setzen sie auf virtuelle Abfangnetze, die Phishing-Mails schnell aufspüren. Damit ist es möglich, betrügerische Webseiten frühzeitig zu sperren, bevor viele irregeführte Bankkunden Gelegenheit hatten, durch sie hinters Licht geführt zu werden.

In den USA haben sich Firmen bereits zur Anti-Phishing Working Group zusammengeschlossen. Auf ihrer Internetseite (www.antiphishing.org) kann man Phishing-Mails melden und nachlesen, welche Phishing-Botschaften schon aufgetreten sind.

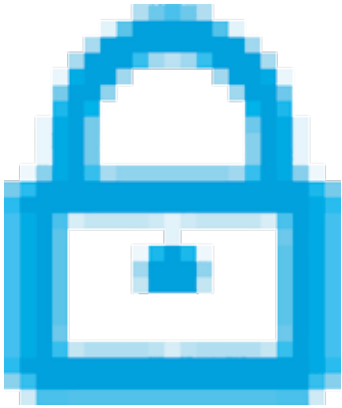
Vertrauen ist gut, Kontrolle ist besser

Bewahren Sie sich bei Aktivitäten im Internet ein gesundes Misstrauen – auch dann, wenn die Inhalte mit bekannten Logos und in vertrauter Gestaltung aufwarten. Darüber hinaus sollten Sie folgendes beachten:

- Vergewissern Sie sich, mit wem Sie es zu tun haben. Überprüfen Sie die Adressleiste in Ihrem Browser. Bei geringsten Abweichungen sollten Sie stutzig werden. Tragen Sie ständig benötigte Internet-Adressen in die Favoritenliste Ihres Browsers ein.
- Klicken Sie nicht auf den angegebenen Link in einer übersandten E-Mail. Versuchen Sie stattdessen, die in der E-Mail angegebenen Seiten direkt über die Startseite Ihrer Bank zu erreichen.
- Kreditinstitute fordern grundsätzlich keine vertraulichen Daten per E-Mail oder per Telefon von Ihnen an. Wenn Sie sich unsicher sind, halten Sie Rücksprache mit Ihrer Bank.
- Übermitteln Sie auch keine persönlichen oder vertraulichen Daten (bspw. Passwörter oder Transaktionsnummern) per E-Mail.

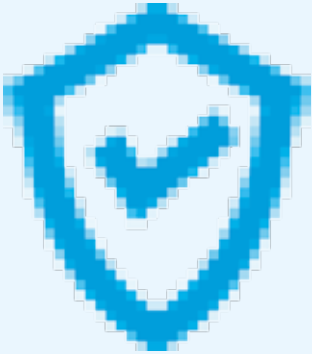
- Folgen Sie Aufforderungen in E-Mails, Programme herunterzuladen, nur dann, wenn Sie die entsprechende Datei auch auf der Internet-Seite des Unternehmens finden (starten Sie keinen Download über den direkten Link). Öffnen Sie insbesondere keine angehängten Dateien!
- Geben Sie persönliche Daten nur bei gewohntem Ablauf innerhalb der Online-Banking-Anwendung Ihres Kreditinstituts an. Sollte Ihnen etwas merkwürdig vorkommen, beenden Sie die Verbindung und versuchen Sie es erneut. Veränderungen sollten Sie misstrauisch machen.
- Beenden Sie die Online-Sitzung bei Ihrer Bank, indem Sie sich abmelden. Schließen Sie nicht lediglich das Browserfenster und wechseln Sie vor Ihrer Abmeldung nicht auf eine andere Internet-Seite.
- Kontrollieren Sie regelmäßig Ihren Kontostand sowie Ihre Kontobewegungen. So können Sie schnell reagieren, falls ungewollte Aktionen stattgefunden haben.
- Rufen Sie sensible Daten nicht über einen fremden WLAN-Zugang (z. B. öffentlicher Hotspot) ab.
- PIN und TAN sollten Sie nur dann eingeben, wenn eine gesicherte Verbindung mit Ihrem Browser hergestellt ist. Diese erkennen Sie an folgenden Merkmalen.

  - Die Adresszeile beginnt mit https://
  - Im Browserfenster erscheint ein kleines Icon, z. B. in Form eines Vorhängeschlosses, das den jeweiligen Sicherheitsstatus symbolisiert („geschlossen“ bzw. „geöffnet“).



- Falls Sie externe Zugangssoftware nutzen, so stellen Sie sicher, dass es sich dabei um die offizielle Version Ihrer Bank handelt.
- Nutzen Sie Funktastaturen nur dann für das Online-Banking, wenn diese über eine eingebaute Verschlüsselung verfügen.
- Benutzen Sie als Passwort eine Kombination aus Zahlen und Buchstaben, am besten noch mit Groß- und Kleinschreibung sowie, wenn möglich, mit Sonderzeichen. Bestehende Begriffe können mit entsprechenden Programmen erraten werden. Ändern Sie Ihre Passwörter regelmäßig (etwa alle ein bis drei Monate).
- Benutzen Sie Passwörter nicht mehrmals für unterschiedliche Zugänge. Insbesondere unseriöse Anbieter, bei denen eine Registrierung notwendig ist, könnten so an vertrauliche Daten gelangen.
- Vernichten Sie nicht mehr benötigte Dokumente, beispielsweise die Zugangsdaten Ihrer Bank oder bewahren Sie diese an einem sicheren, nicht zugänglichen Ort auf (Safe oder ähnliches).
- Ein hohes Maß an Sicherheit bieten alle Homebanking-Programme, die eine Offline-Eingabe ermöglichen.
- Noch besser: Sie entscheiden sich für HBCI-Banking mit Chipkarte und Kartenlesegerät.

- Speichern Sie vertrauliche Daten nicht ungeschützt auf der Festplatte Ihres Computers. Sollten Sie ein Homebanking-Programm benutzen, werden die Kontodaten zumeist verschlüsselt abgelegt. Informieren Sie sich hier bei dem jeweiligen Hersteller der Software.
- Halten Sie Ihren Rechner auf dem neuesten Stand. Nutzen Sie die Update-Funktion des Herstellers Ihres Betriebssystems. Microsoft bietet die Möglichkeit, den Rechner auf aktuelle Schwächen zu prüfen und entsprechend zu aktualisieren.
- Passen Sie die Sicherheitseinstellungen in Ihrem Browser Ihren Bedürfnissen an. Bedenken Sie allerdings, dass sich strikte Einstellungen auf Ihre „Bewegungsfreiheit“ im Netz auswirken können. Verhindern Sie beispielsweise das Anlegen von Cookies, können Sie unter Umständen Bestellvorgänge bei einem Online-Shop nicht vornehmen.
- Verwenden Sie aktuelle Virenscanner und zusätzliche Sicherheitssoftware wie z. B. Firewalls.
- Weitere Informationen zu den Sicherheitseinstellungen von Browsern finden Sie auf den Seiten von Heise Security (https://www.heise.de/security/dienste/Browsercheck-2107.html).
- Außerdem sollten Sie Bankgeschäfte nur an Rechnern von Personen durchführen, denen Sie vertrauen. Es gibt Programme oder technische Einrichtungen, die Ihre Eingaben mitloggen können, ohne dass Sie es merken.



Nützliche Link-Tipps

Bundesamt für Sicherheit in der Informationstechnik:
www.bsi-fuer-buerger.de

Polizeiliche Kriminalprävention der Länder und des Bundes:
www.polizei-beratung.de

Informationsseite für Onlinetipps gegen Straftaten und Abzocke im Internet und am Telefon:
www.computerbetrug.de

Bundesverband der Deutschen Volksbanken und Raiffeisenbanken e. V. :
www.bvr.de

Bundesverband deutscher Banken e. V. :
www.bankenverband.de

Bundesverband Öffentlicher Banken Deutschlands e. V.:
www.voeb.de

Deutscher Sparkassen- und Giroverband e. V. :
www.dsgv.de

Unser Programm:
Helfen – Beraten – Vorbeugen

Aufgaben des WEISSEN RINGS sind:

- Hilfe für Personen, die durch eine rechtswidrige Straftat unmittelbar oder mittelbar geschädigt wurden. Die Unterstützung kann sowohl durch immaterielle als auch durch materielle Leistungen erfolgen
- Öffentliches Eintreten für die Belange der Geschädigten. Ziel ist die nachhaltige Verbesserung der rechtlichen und sozialen Situation von Kriminalitätsopfern und ihrer Angehörigen
- Maßnahmen zur Unterstützung der Kriminalitätsvorbeugung
- Unterstützung von Projekten der Schadenswiedergutmachung und des Täter-Opfer-Ausgleichs

Der WEISSE RING kann u. a. helfen durch:

- Menschlichen Beistand und persönliche Betreuung nach der Straftat
- Begleitung zu Terminen bei Polizei, Staatsanwaltschaft und Gericht
- Hilfestellung im Umgang mit weiteren Behörden
- Vermittlung von Hilfen durch andere Organisationen
- Hilfeschecks für eine für das Opfer jeweils kostenlose frei wählbare anwaltliche bzw. psychotherapeutische Erstberatung sowie für eine rechtsmedizinische Untersuchung
- Übernahme von Anwaltskosten, insbesondere
  - zur Wahrung von Opferschutzrechten im Strafverfahren
  - zur Durchsetzung von Ansprüchen nach dem Opferentschädigungsgesetz
- Erholungsmaßnahmen für Opfer und deren Angehörige in bestimmten Fällen
- Finanzielle Unterstützung zur Überbrückung tatbedingter Notlagen
- **Bundesweites Opfer-Telefon 116 006**

Ihre Unterstützung ist wichtig

Im Auftrag von Menschen, denen das Schicksal von Kriminalitätsopfern wichtig ist, gibt der WEISSE RING Opfern und ihren Angehörigen durch seine rund 3.200 ehrenamtlichen Helferinnen und Helfern wieder Mut und neue Hoffnung. Gemeinsam entstehen so Tag für Tag an unzähligen Orten Mitmenschlichkeit und Lebenshilfe.

Die Mitgliedschaft in dieser Bürgerinitiative ist ein sinnvolles und zweckmäßiges Mittel, diese wichtige Arbeit zu ermöglichen.

Der monatliche Mindestbeitrag beträgt

für die Einzelmitgliedschaft	2,50 Euro
für Ehepaare	3,75 Euro
für Jugendliche	1,25 Euro

Jedes neue Mitglied stärkt die Stimme der Opfer. Hilfe für Kriminalitätsopfer geht uns alle an. Jeder von uns kann schon morgen selbst zu den Betroffenen gehören.

Auch jede Spende, egal in welcher Höhe, hilft. Danke!

Spendenkonto WEISSER RING: 34 34 34
Deutsche Bank Mainz (BLZ 550 700 40)
BIC: DEUTDE5MXXX
IBAN: DE26 5507 0040 0034 3434 00

www.weisser-ring.de

Bitte senden an: WEISSER RING e. V., Weberstraße 16, 55130 Mainz

Beitrittserklärung

(Bitte in Blockbuchstaben ausfüllen)

WEISSER RING

Familienname | Vorname

Straße / Hausnummer

PLZ / Wohnort

Geburtsdatum | Geburtsort

Staatsangehörigkeit | Beruf

Telefon privat | Telefon dienstlich

Monatliche Mindestbeiträge für die Mitgliedschaft im WEISSEN RING:
€ 2,50 (Einzelmitgliedschaft) • € 3,75 (Ehepaare) • € 1,25 (Jugendmitgliedschaft)

Einzelmitgliedschaft
Ich unterstütze den WEISSEN RING mit einem Monatsbeitrag von:
☐ € 2,50 ☐ € 3,75 ☐ € 5,00 ☐ € _____

Mitgliedschaft für Ehepaare
Wir unterstützen den WEISSEN RING mit einem Monatsbeitrag von:
☐ € 3,75 ☐ € 5,00 ☐ € 10,00 ☐ € _____

Zweite Beitrittserklärung für Ehepartner ☐ liegt bei ☐ wird erbeten

Jugendmitgliedschaft (Schüler/innen, Studierende, Auszubildende, FSJ, FÖJ und BFD – Nachweis wird erbeten)
Ich unterstütze den WEISSEN RING mit einem Monatsbeitrag von:
☐ € 1,25 ☐ € 2,50 ☐ € 3,75 ☐ € _____

Jährliche Zuwendungsbestätigung erwünscht ☐ ja ☐ nein

Geworben durch Außenstelle/Mitarbeiter/in: _____

Der Jahresbeitrag soll durch Lastschrift eingezogen werden.
☐ vierteljährlich ☐ halbjährlich ☐ jährlich

SEPA-Lastschriftmandat Gläubiger-Identifikationsnummer: DE07ZZZ00000148641. Die Mandatsreferenz wird separat mitgeteilt. Ich/wir ermächtige/n den WEISSEN RING e. V., meinen/unseren Mitgliedsbeitrag von meinem/unserem Konto mittels Lastschrift einzuziehen. Zugleich weise/n ich/wir mein/unser Kreditinstitut an, die vom WEISSEN RING e. V. auf mein/unser Konto gezogenen Lastschriften einzulösen.
Hinweis: Ich/wir kann/können innerhalb von acht Wochen, beginnend mit dem Belastungsdatum, die Erstattung des belasteten Betrages verlangen. Es gelten dabei die mit meinem/unserem Kreditinstitut vereinbarten Bedingungen.

_ _ _ _ _ _ _ _ | _ _ _ | DE _ _ | _ _ _ _ | _ _ _ _ | _ _ _ _ | _ _ _ _ | _ _

BIC | IBAN

Kreditinstitut | in

Ort/Datum | Unterschrift

WR-Akt.-Nr. 1941

Rückantwort passend für Fensterkuvert DIN Lang

Familienname

Vorname

Straße / Hausnummer

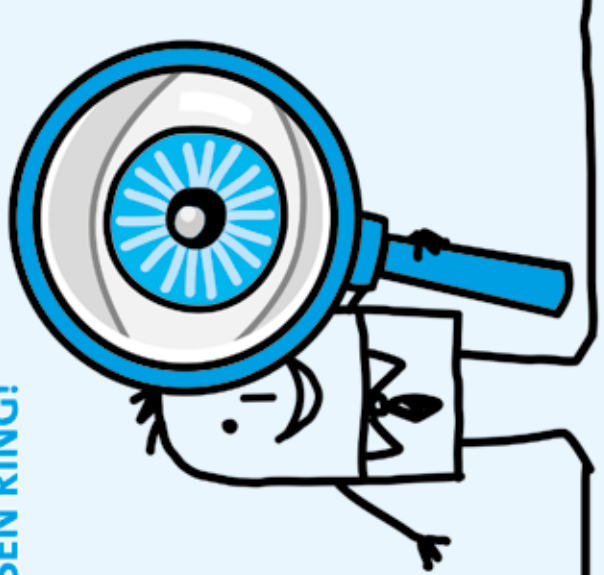
PLZ / Wohnort

WEISSER RING e. V.
Bundesgeschäftsstelle
Weberstraße 16
55130 Mainz

WEISSER RING e. V. - Wir helfen Kriminalitätsopfern.

Wir suchen Sie!

Werden Sie jetzt Mitglied beim WEISSEN RING!



WR-Artikel-Nr. 1058 / 2017, 20.000 Exemplare