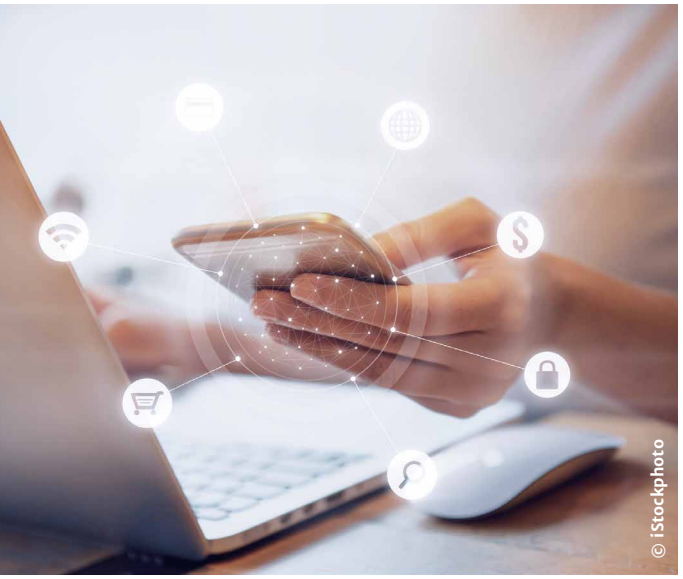


Der WEISSE RING hilft

Wer im Internet Opfer einer Straftat geworden ist, kann sich an den WEISSEN RING wenden. Über das Opfer-Telefon, die Onlineberatung oder eine der 420 Außenstellen hilft der WEISSE RING – anonym und kostenlos!

Der WEISSE RING hilft durch:

- Aufklärung über Internetkriminalität
- Ratschläge zu konkreten Präventionsmaßnahmen
- Menschlichen Beistand und persönliche Betreuung nach einer Straftat
- Begleitung zu Terminen bei Behörden wie Polizei oder Gericht
- Hilfeschecks für eine psychotraumatologische oder anwaltliche Erstberatung
- Vermittlung von Hilfen anderer Anlaufstellen

WEISSER RING
Wir helfen Kriminalitätsopfern.

Opfer-Telefon:

116 006

(bundesweit kostenfrei)

Onlineberatung:

www.weisser-ring.de/hilfe/onlineberatung

www.weisser-ring.de
www.youtube.com/weisserringev
www.facebook.com/weisserring
WEISSER RING e. V. • Bundesgeschäftsstelle
Weberstraße 16 • 55130 Mainz • Germany
info@weisser-ring.de

Februar 2018
Artikelnummer: Internetkriminalität 2070
Gefahren und Schutz im Web

Internetkriminalität

Gefahren und Schutz im Web

Online-Verbrechen haben handfeste Auswirkungen

Laut der ARD/ZDF-Onlinestudie nutzten im Jahr 2017 allein in Deutschland rund 62 Millionen Personen das Internet. Dabei wurde jeder zweite Internetnutzer schon einmal Opfer von Kriminalität im Netz. Das ist das Ergebnis einer repräsentativen Umfrage des Digitalverbandes Bitkom. Ob Erpressung mit blockierten Daten, Betrug beim Online-Shopping, Identitätsmissbrauch, Verleumdung oder Mobbing – von Kriminalität im Netz sind immer mehr Menschen betroffen und sie verursacht erheblichen Schaden. Fast die Hälfte der Betroffenen trägt Bitkom zufolge einen finanziellen Schaden davon. Opfer fühlen sich aber auch machtlos, schämen sich und leiden oft unter psychischen Folgen.

Formen von Kriminalität im Internet

Phishing: Unter dem Begriff Phishing (engl. für Angeln) versteht man Versuche, an persönliche Daten eines Internet-Benutzers zu gelangen und damit Identitätsdiebstahl zu begehen. Die Täter versenden sogenannte Phishing-Mails oder treten in Sozialen Netzwerken als vermeintlich vertrauenswürdige Person auf. Ziel der Täter ist dabei, persönliche Daten wie Passwörter, Adress- und Bankdaten und andere vertrauliche Informationen der Opfer zu erhalten. Die Daten werden später für weitere kriminelle Handlungen eingesetzt, die dem Opfer finanzielle Schäden bereiten.

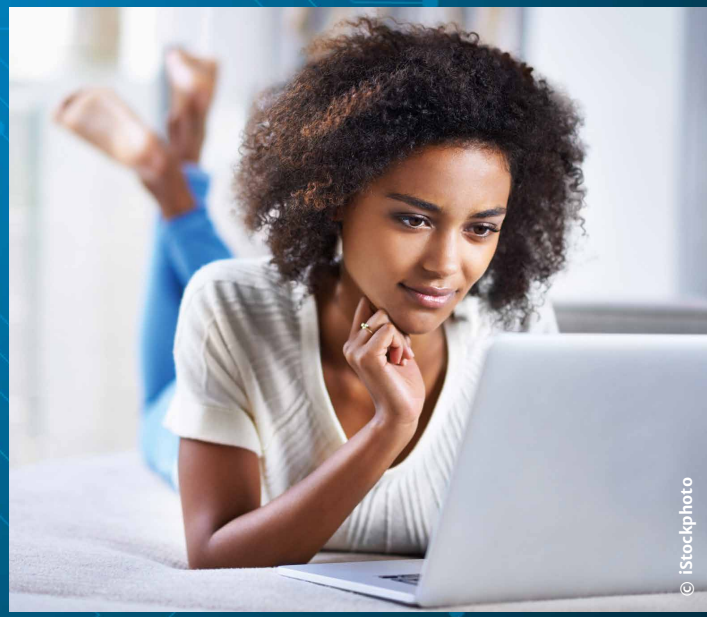
Fake-Shops: Kriminelle richten unter bekannten, aber leicht veränderten Internetadressen Webshops ein und bieten dort vermeintlich hochwertige Markenartikel günstig gegen Vorkasse an. Die Produkte werden nach Eingang der Zahlung jedoch nicht geliefert.

Schadsoftware/ Trojanische Pferde: Ein schädliches Programm wird in einem nützlichen Programm versteckt und so auf dem Computer, Handy oder Tablet installiert. Es kann dann unbemerkt Passwörter und Daten ausspähen, verändern, löschen oder an den Absender verschicken. Außerdem kann ein eingeschleustes Programm die Daten auf einem Gerät verschlüsseln. Damit der Nutzer wieder an diese Daten gelangen kann, wird er vom Täter aufgefordert, Lösegeld zu bezahlen.

Botnetz: Durch ein verstecktes Programm kann der eigene Computer unwissentlich Teil eines kriminellen Netzwerks werden. Ein Roboterprogramm, kurz Bot, späht dabei unbemerkt Daten aus, versendet Spam an andere Nutzer oder führt für Kriminelle Cyberangriffe gegen Unternehmen durch.

Cybermobbing: Beleidigen, bloßstellen, bedrohen oder belästigen einer Person via Computer oder Smartphone über einen längeren Zeitraum – das bezeichnet man als Cybermobbing. Betroffen sind sowohl Kinder und Jugendliche als auch Erwachsene im Privatleben und in der Arbeitswelt. Beleidigung, Verleumdung und Bedrohung sind meistens Teil des Mobbings und können einen Straftatbestand darstellen.

Cybergrooming: Erwachsene kontaktieren Kinder und Jugendliche über das Internet mit dem Ziel, sie zu sexuellen Handlungen zu bringen und zu missbrauchen. Dabei werden Minderjährige häufig dazu aufgefordert, sexuelle Handlungen an sich vorzunehmen oder es wird ihnen pornographisches Material präsentiert.



© iStockphoto

Prävention: So schützen Sie sich!

Einen hundertprozentigen Schutz gegen Gefahren im Internet gibt es leider nicht. Aber jeder kann etwas für die eigene Sicherheit im Netz tun:

Updates und Software: Betriebssysteme Ihrer Rechner, Smartphones und Tablets sollten stets mit neuen Updates des Herstellers versehen sein. Auch aktuelle Virenscanner und zusätzliche Sicherheitssoftware wie Firewalls sind wichtige Präventionsmaßnahmen.

Passwörter: Für unterschiedliche Zugänge wie beispielsweise E-Mail-Programme und Soziale Netzwerke sollten immer verschiedene Passwörter verwendet werden. Passwörter sollten immer aus einer Kombination von Buchstaben, Zahlen und Sonderzeichen bestehen, mindestens acht Zeichen haben und regelmäßig gewechselt werden.

Öffentliche WLAN-Netzwerke meiden: Wer öffentliche WLAN-Netzwerke nutzt, setzt sich dem Risiko aus, dass Daten unverschlüsselt übertragen und abgefangen werden. Unbekannte WLAN-Netzwerke sollten deshalb möglichst nicht genutzt werden.

Verhalten: Wichtig ist auch das eigene Verhalten im Netz. Jeder hinterlässt beim Surfen eine Datenspur. Je mehr Daten Sie öffentlich über sich preisgegeben, desto einfacher kann damit Missbrauch betrieben werden. Mit eigenen Daten wie Fotos, Adressen und Telefonnummern sollte zurückhaltend umgegangen werden. Es ist auch sinnvoll, nicht alle Links anzuklicken oder Anhänge zu öffnen, die man per E-Mail oder in Sozialen Netzwerken erhält. Hinterfragen Sie kritisch den Absender. Handeln Sie nicht unüberlegt und seien Sie vorsichtig.

Auffälligkeiten, Verstöße und Straftaten melden: Alle kriminellen Vorfälle oder der Verdacht darauf sollten beim Betreiber einer Internetseite, eines Netzwerks und/oder der Polizei gemeldet werden.