Über Kaspersky Lab

Kaspersky Lab reagiert im weltweiten Vergleich von Antivirus-Herstellern meist am schnellsten auf IT-Sicherheitsbedrohungen wie Viren, Spyware, Crimeware, Hacker, Phishing-Attacken und Spam. Die Produkte des global agierenden Unternehmens mit Hauptsitz in Moskau haben sich sowohl bei Endkunden als auch bei KMUs, Großunternehmen und im mobilen Umfeld durch ihre erstklassigen Erkennungsraten und minimalen Reaktionszeiten einen Namen gemacht. Neben den Stand-Alone-Lösungen des Security-Experten ist Kaspersky-Technologie Bestandteil vieler Produkte und Dienstleistungen führender IT-Sicherheitsunternehmen. Mit den Kaspersky Hosted Security Services bietet das Unternehmen darüber hinaus Dienstleistungen im Bereich Malware- und Spam-Schutz sowie Content-Kontrolle für Unternehmen jeder Größe an.

Weitere Details zum Unternehmen sind unter www.kaspersky.de zu finden. Aktuelles zu Viren, Spyware und Spam sowie Informationen zu anderen IT-Sicherheitsproblemen und Trends sind unter www.viruslist.de abrufbar.

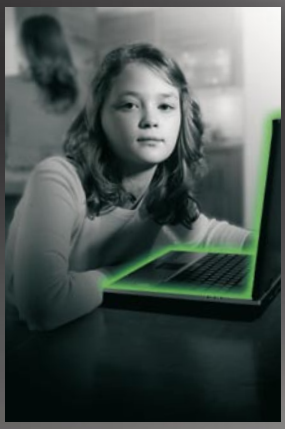
www.stop-cybercrime.de

Kaspersky Labs GmbH
Steinheilstrasse 13
D-85053 Ingolstadt
Deutschland

Tel: +49 (0) 841 98 18 90
Fax: +49 (0) 841 98 189 100

www.kaspersky.de

KASPERSKY lab

Ratgeber zum Schutz vor Cyberkriminalität

Inhaltsverzeichnis

Wozu dieser Ratgeber?

Diese Anleitung soll Ihnen helfen, sich vor Cyberangriffen zu schützen. Zu solchen Cyberangriffen zählen u. a. **Viren, Würmer, Trojaner, Hacker**- und **Phishing**-Angriffe. Sie sind heute nicht nur raffinierter als je zuvor – sie sind auch zahlreicher. Viele dieser Bedrohungen zielen darauf ab, Ihre Identität zu stehlen, Ihre persönlichen Daten zu sammeln und an Ihr Geld zu gelangen.

Doch auch wenn die Risiken durch Online-Angriffe ständig zunehmen – wenn Sie sich an die einfachen Vorsichtsmaßnahmen dieser Anleitung halten, gibt es keinen Grund, warum das Surfen im Internet nicht auch weiterhin unterhaltsam, produktiv und sorglos bleiben sollte.

Worin besteht das Risiko?

Sobald Sie Ihren PC mit dem Internet verbinden, wird er zu einem potenziellen Ziel für Cyberkriminelle. Genauso wie Einbrecher bei einem ungesicherten Haus leichtes Spiel haben, ist ein ungeschützter PC wie eine offene Einladung an Autoren von **Malware** (kurz für Malicious Software) sowie an die für Malware zahlenden Cyberkriminellen.

Noch vor wenigen Jahren handelte es sich bei Viren, Würmern und auch bei Hacker-Angriffen meist nur um eine Art „Cyber-Vandalismus“, eine rücksichtslose Form der Selbstdarstellung mithilfe von Computertechnologie. Kaum eines dieser Programme wurde gezielt dazu entwickelt, um Schäden zu verursachen; dennoch führte eine kleine Anzahl dieser Programme zu Datenschäden oder machten den Computer unbrauchbar (meist eher als Nebeneffekt). Bei den bösartigen Programmen, die zu jener Zeit in Umlauf waren, handelte es sich größtenteils um Viren und Würmer.

Heute dagegen geht die größte Gefahr von der Cyberkriminalität aus. Kriminelle haben erkannt, dass sich in unserer allseits vernetzten Welt mit bösartigem Code große Summen ergaunern lassen und nutzen ihn, um vertrauliche Daten (Benutzernamen, Kennwörter, PINs usw.) zu stehlen.

Den Großteil der bösartigen Programme machen heute Trojaner aus. Man unterscheidet zwischen vielen unterschiedlichen Arten von Trojanern: Einige spionieren aus, welche Tasten Sie drücken, oder fertigen Screenshots vom Inhalt Ihres Bildschirms, während Sie eine Online-Banking-Seite besuchen. Andere laden zusätzlichen bösartigen Code herunter oder verschaffen einem entfernten Hacker Zugriff auf Ihren Computer. Doch sie alle haben etwas gemeinsam: Sie ermöglichen Cyberkriminellen, Ihre vertraulichen Daten zu sammeln und damit an Ihr Geld zu gelangen.

Bei den meisten bösartigen Programmen handelt es sich um Trojaner, die vertrauliche Daten und damit Ihr Geld anvisieren.

Was können schädliche Programme anrichten?

Cyberbedrohungen werden nicht nur immer raffinierter, sondern nehmen auch ständig zu: Unser Antiviruslabor verzeichnet derzeit über 17.000 neue Internetbedrohungen pro Tag.

Wie andere Software auch, verhalten sich bösartige Programme auf eine bestimmte Weise und führen spezifische Funktionen aus. Sie unterliegen denselben Beschränkungen wie jedes andere Programm. Was sie tun, hängt davon ab, wofür der Autor der Malware sie programmiert hat.

Viele ältere Viren enthielten keine Schadfunktionen; sie waren lediglich zur Verbreitung bestimmt. Manche verursachten (als Resultat schlechter Programmierung) unbeabsichtigte Nebeneffekte wie in einigen wenigen Fällen die Löschung oder Beschädigung von Dateien. Diese Programme konnten zwar störend sein oder auch Datenverluste verursachen, ihr Zweck war jedoch selten die Erfassung der Daten für eine spätere Nutzung.

Das hat sich grundlegend geändert. Heute besteht das Ziel bösartiger Programme in der Regel im Datendiebstahl. Daher spricht man bei vielen Trojanern auch von **Spyware**: Sie installieren sich ohne Ihr Wissen oder Ihre Zustimmung und verfolgen ihre Aktionen Tag für Tag. Dabei verschleiern sie ihre Anwesenheit mithilfe von sogenannten **Rootkits**. So läuft alles normal weiter, und Sie schöpfen keinen Verdacht.

Kaspersky Lab verzeichnet täglich über 17.000 neue Internetbedrohungen

Heute werden Spyware-Programme ohne Ihr Wissen oder Ihre Zustimmung installiert. Sie bemerken nicht, wie Ihre persönlichen Daten gesammelt werden.

Hacker-Angriffe

Die heutigen Anwendungen sind äußerst komplex und aus Tausenden von Codezeilen zusammengesetzt. Und da sie von Menschen geschrieben sind, sind sie nicht immer fehlerfrei. Es ist daher nicht überraschend, dass sie auch sicherheitskritische Programmierfehler, so genannte **Schwachstellen**, enthalten. Diese Sicherheitslücken werden erstens von Hackern genutzt, um in Systeme einzudringen, und zweitens von Autoren von bösartigem Code, um ihre Programme automatisch auf Ihrem Computer zu starten.

Das Wort „Hacker“ wurde ursprünglich zur Bezeichnung eines cleveren Programmierers verwendet. Heute bezeichnet man damit unter anderem Personen, die durch Ausnutzung von Sicherheitslücken in ein Computersystem eindringen. Es handelt sich sozusagen um einen elektronischen Einbruch. Hacker dringen immer wieder sowohl in einzelne Computer als auch in große Netzwerke ein. Sobald sie sich Zugriff auf ein System verschafft haben, installieren sie bösartige Programme, stehlen vertrauliche Daten oder benutzen infizierte Computer, um Spam zu verteilen. Zudem können sie auch die Webserver anderer Unternehmen mit Datenverkehr überschwemmen: Solche DoS-Angriffe (**Denial of Service**) haben das Ziel, eine Website zu überlasten, so dass diese nicht mehr erreichbar ist. Damit kann das entsprechende Unternehmen geschädigt und auch erpresst werden.

Da Cyberkriminelle von ihrer investierten Zeit und Mühe maximal profitieren wollen, zielen sie auf die am meisten verbreiteten Systeme ab. Daher auch die starke Fokussierung von Hackern auf Microsoft Windows: Es ist das weltweit am meisten verwendete Betriebssystem.

Hacker agieren wie elektronische Einbrecher: Sie nutzen die Sicherheitslücken in normalen Programmen, die so genannten Schwachstellen, um in Ihren Computer einzudringen.

Wie kann ich mich vor bösartigem Code und vor Hacker-Angriffen schützen?

Sie können verschiedene Maßnahmen ergreifen, um Ihren Computer vor den heutigen Cyberbedrohungen zu schützen. Durch Beachtung der einfachen Regeln unten können Sie das Risiko von Angriffen minimieren.

- Schützen Sie Ihren Computer, indem Sie Internet-Sicherheitssoftware installieren.
- Stellen Sie sicher, dass Ihre Software sich regelmäßig automatisch aktualisiert oder führen Sie Updates selbst durch (mindestens einmal pro Tag).
- Installieren Sie Sicherheitspatches für Ihr Betriebssystem und Ihre Anwendungen. Wenn Sie Windows verwenden, aktivieren Sie einfach „Automatische Aktualisierungen“. Denken Sie auch daran, Microsoft Office zu aktualisieren.
- Aktualisieren Sie auch Ihre sonstigen Anwendungen, beispielsweise Ihren E-Mail-Client und Ihren Web-Browser.
- Wenn Sie eine E-Mail mit angehängter Datei erhalten (z. B. Word-Dokument, Excel-Tabelle oder EXE-Dateie), öffnen Sie diese nur, wenn Sie den Absender kennen und diese Datei auch erwarten. Öffnen Sie NIE den Anhang einer unerwünschten E-Mail (Spam). Dasselbe gilt für E-Mail- oder IM (Instant Messaging)-Nachrichten, die Links enthalten.
- Benutzen Sie das Administratorkonto nur dann, wenn Sie auf Ihrem Computer Software installieren oder Systemänderungen vornehmen. Richten Sie für den täglichen Gebrauch ein separates Benutzerkonto mit eingeschränkten Zugriffsrechten ein (über die Option „Benutzerkonten“ unter „Systemsteuerung“). Auf diese Weise schränken Sie den Zugriff bösartiger Programme auf wertvolle Systemdaten ein.
- Führen Sie regelmäßig Backups Ihrer Daten auf einer CD, DVD oder einem externen USB-Laufwerk durch. Falls Ihre Dateien von einem bösartigen Programm beschädigt oder verschlüsselt wurden, können Sie sie aus dem zuvor angelegten Backup zurückkopieren.

Schutz vor bösartigem Code und Hacker-Angriffen:

✓ **Installieren Sie Internet-Sicherheitssoftware.**
✓ **Installieren Sie Sicherheitspatches.**
✓ **Seien Sie vorsichtig bei unerwünschten E-Mail- oder IM-Nachrichten.**
✓ **Gehen Sie vorsichtig vor, wenn Sie sich mit Administratorrechten anmelden.**
✓ **Führen Sie Backups Ihrer Daten durch.**

Was bedeutet Phishing?

Unter „Phishing“ versteht man Versuche, Ihre Identität zu stehlen, Ihre persönlichen Daten zu sammeln und damit an Ihr Geld zu gelangen.

Cyberkriminelle senden Ihnen zunächst eine E-Mail, die einen Link enthält. Wenn Sie auf den Link klicken, werden Sie zu einer gefälschten Website geleitet, die genau wie die Website zum Beispiel Ihrer Bank aussieht. Sie sollen dann dazu verleitet werden, Ihren Benutzernamen, Ihr Kennwort oder Ihre PIN einzugeben. Diese Daten werden von den Cyberkriminellen erfasst und dazu verwendet, um Geld von Ihrem Konto abzuheben.

Meist versenden die Cyberkriminellen zu diesem Zweck eine große Anzahl an E-Mails, die so aussehen, als kämen sie von einer Bank (oder von einer bekannten Firma). Viele, die diese E-Mail erhalten, sind natürlich nicht Kunden der besagten Bank. Doch für die Cyberkriminellen reicht es bereits aus, wenn ein kleiner Prozentsatz der Empfänger dieser E-Mail auf den Betrug hereinfällt, um an Geld zu kommen.

Mit Phishing-E-Mails sollen Sie hinters Licht geführt werden, indem das Design und das Logo der Originalbank nachgeahmt, ein der URL der Originalbank ähnlicher Link verwendet oder Ihr Name genannt wird, um so den Anschein einer an Sie persönlich gerichteten E-Mail zu wecken. Meist wird in diesen E-Mails ein falscher Grund für das Schreiben genannt, und Sie werden gebeten, personenbezogene Details anzugeben: Die Bank führe stichprobenartige Sicherheitsprüfungen durch oder habe Änderungen an ihrer Infrastruktur vorgenommen und benötige zu diesem Zweck eine erneute Bestätigung der Kundendaten.

Oft heben Cyberkriminelle nur einen relativ kleinen Betrag ab, damit kein Verdacht entsteht. Da es dabei meist viele potenzielle Opfer gibt, bedeutet ein kleiner Betrag von jedem Opfer einen beträchtlichen Gewinn für die Cyberkriminellen.

Phishing-E-Mails geben vor, von einer Bank oder einer anderen bekannten Firma zu stammen. Sie enthalten in der Regel einen Link, über den Sie auf eine gefälschte Website geleitet werden. Dort sollen Sie dazu gebracht werden, Ihre vertraulichen Daten einzugeben, damit Cyberkriminelle Geld von Ihrem Bankkonto abheben können.

Sandra ist geschützt.

Sandra organisiert ihren Alltag im Internet. Hier kauft sie ein, erledigt ihre Bankgeschäfte und hält Kontakt mit Freunden. Auf Ihrem PC speichert Sie Familienfotos und andere persönliche Daten. Wegen Cybercrime macht sie sich keine Sorgen, auch wenn Kriminelle im Internet täglich mit über 17.000 neuen Bedrohungen auf ihre persönlichen Daten und Passwörter aus sind. Online-Betrug, Identitätsdiebstahl oder das Ausspionieren von Passwörtern – all das bereitet Sandra keine schlaflosen Nächte.

Wie kann ich mich vor Phishing-Angriffen schützen?

Befolgen Sie die oben genannten Hinweise zum Schutz vor bösartigem Code und vor Hacker-Angriffen. Zusätzlich können Sie durch Beachtung der folgenden Regeln das Risiko minimieren, einem Phishing-Angriff zum Opfer zu fallen.

- Geben Sie keine persönlichen Informationen preis, wenn Sie in einer E-Mail dazu aufgefordert werden. Es ist äußerst unwahrscheinlich, dass Ihre Bank Sie per E-Mail um die Angabe solcher Informationen bittet. Wenn eine E-Mail-Nachricht vorgeblich von Ihrer Bank stammt, rufen Sie diese zur Überprüfung an.
- Klicken Sie nicht auf Links in HTML-E-Mails, um auf eine Website zu gelangen. Cyberkriminelle können die URL einer gefälschten Website hinter einem scheinbar harmlosen Link verbergen. Geben Sie die URL stattdessen selbst in die Adresszeile Ihres Webbrowsers ein. Oder konfigurieren Sie Ihr E-Mail-Programm so, dass es nur Klartext verwendet, da dieser Trick dann nicht funktioniert.
- Füllen Sie keine Formulare in E-Mails aus, in denen Sie Ihre persönlichen Informationen angeben sollen. Geben Sie solche Daten nur auf einer sicheren Website ein. Überprüfen Sie, ob die URL mit „https://“ beginnt, und achten Sie auf das Schloss-Symbol in der rechten unteren Ecke Ihres Webbrowsers. Mit einem Doppelklick auf das Schloss überprüfen Sie, ob die Adresse im Sicherheitszertifikat mit der in der Adresszeile des Webbrowsers übereinstimmt. Sollten Sie Zweifel haben, führen Sie Ihre Banktransaktionen telefonisch durch.
- Überprüfen Sie Ihre Bankkonten regelmäßig (einschließlich Debit- und Kreditkarten, Kontoauszüge usw.) und prüfen Sie, ob alle Transaktionen von Ihnen veranlasst wurden. Informieren Sie Ihre Bank umgehend über verdächtige Aktivitäten.
- Seien Sie vorsichtig bei E-Mails, die nicht an Sie persönlich gerichtet sind, z. B. E-Mails mit der Anrede „Sehr geehrter Kunde“ oder ähnlichem.
- Seien Sie vorsichtig, wenn Sie nicht der einzige Empfänger sind. In dem sehr unwahrscheinlichen Fall, dass Ihre Bank mit Ihnen per E-Mail über Ihr persönliches Konto kommuniziert, wird sie diese E-Mail nicht an andere Personen schicken.
- Seien Sie vorsichtig bei auffälligen Rechtschreib-, Grammatik- oder Satzbaufehlern und sonstigen sprachlichen Schwächen.

So schützen Sie sich vor Phishing-Angriffen:

- ✓ **Klicken Sie nicht auf Links in E-Mail-Nachrichten.**
- ✓ **Geben Sie vertrauliche Daten nur auf einer sicheren Website ein.**
- ✓ **Überprüfen Sie Ihre Bankkonten regelmäßig, und informieren Sie Ihre Bank über verdächtige Aktivitäten**
- ✓ **Achten Sie auf Anzeichen für Phishing-E-Mails:**
  - **E-Mails, die nicht an Sie persönlich gerichtet sind.**
  - **E-Mails, bei denen Sie nicht der einzige Empfänger sind.**
  - **E-Mails mit auffälligen Rechtschreib-, Grammatik- oder Satzbaufehlern und sonstigen sprachlichen Schwächen**
- ✓ **Beachten Sie die Hinweise zum Schutz vor bösartigem Code und Hacker-Angriffen.**

Können meine Daten durch ein bösartiges Programm beschädigt werden?

Ja, einige Cyberkriminelle versuchen, mithilfe von **Ransomware**-Programmen Geld von ihren Opfern zu erpressen. Mit diesen Programmen werden Ihre Daten verschlüsselt, und auf Ihrer Festplatte wird eine sogenannte Readme-Datei mit Informationen dazu erstellt, wie Sie mit den Betrügern Kontakt aufnehmen können. Es wird versprochen, dass Sie Ihre Daten zurückbekommen, wenn Sie über ein Online-Bezahlsystem wie „e-gold“ oder „WebMoney“ Geld bezahlen.

Manche Cyberkriminelle verwenden Ransomware-Programme, um Ihre Daten zu verschlüsseln. Sie fordern Geld für die Anleitung, wie Sie Ihre Daten zurückbekommen.

Wie kann ich mich vor Ransomware schützen?

Beachten Sie die Hinweise zu Ihrem Schutz vor bösartigem Code und Hacker-Angriffen. Zusätzlich können Sie durch Beachtung der folgenden Regeln das Risiko minimieren, einem Ransomware-Angriff zum Opfer zu fallen.

- Sichern Sie Ihre Daten regelmäßig. Bisher konnte Kaspersky Lab alle Daten, die von Ransomware-Programmen verschlüsselt wurden, wiederherstellen. Doch angesichts der immer raffinierteren Verschlüsselungsmethoden von Cyberkriminellen können wir dies für die Zukunft nicht garantieren. Verfügen Sie jedoch über eine Datensicherung, gehen auch keine Daten verloren.
- Zahlen Sie NIE Geld an Cyberkriminelle. Falls Sie nicht über eine Datensicherung verfügen, wenden Sie sich an Ihren Antivirus-Anbieter, da dieser Ihnen möglicherweise bei der Wiederherstellung der Daten helfen kann.

So schützen Sie sich vor Ransomware:

- ✓ **Sichern Sie Ihre Daten.**
- ✓ **Zahlen Sie NIE Geld an Cyberkriminelle.**
- ✓ **Beachten Sie die Hinweise zum Schutz vor bösartigem Code und Hacker-Angriffen.**

Wie schütze ich mein drahtloses Netzwerk?

Die meisten Computer unterstützen drahtlose Verbindungen: Damit können Sie ohne Kabel eine Verbindung zum Internet herstellen. Der offensichtlichste Vorteil besteht darin, dass Sie Ihren Computer überall im Haus oder im Büro verwenden können (vorausgesetzt, Sie befinden sich innerhalb der Reichweite Ihres drahtlosen Routers). Dennoch bestehen potenzielle Risiken, wenn Sie Ihr drahtloses Netzwerk nicht sichern:

1. Daten, die Sie versenden oder empfangen, können von einem Hacker abgefangen werden.
2. Ein Hacker kann sich Zugriff auf Ihr drahtloses Netzwerk verschaffen.
3. Eine andere Person kann Ihren Internetzugang übernehmen.

Wenn Ihr drahtloses Netzwerk nicht gesichert ist, können Hacker die von Ihnen gesendeten Daten abfangen, auf Ihr Netzwerk und über Ihre Verbindung auf das Internet zugreifen.

Mit einigen einfachen Maßnahmen können Sie Ihren drahtlosen Router schützen und solche Risiken minimieren:

- Ändern Sie das Administratorkennwort für Ihren drahtlosen Router. Für einen Hacker ist es nicht schwer, das standardmäßige Kennwort des Herstellers herauszufinden und damit auf Ihr drahtloses Netzwerk zuzugreifen. Vermeiden Sie Kennwörter, die sich einfach erraten lassen, und folgen Sie bei der Wahl des Kennworts den Richtlinien im hinteren Teil dieses Ratgebers.
- Aktivieren Sie die Verschlüsselung: WPA2-Verschlüsselung ist am sichersten. Falls Ihr Gerät diese nicht unterstützt, verwenden Sie WPA. Auf keinen Fall sollten Sie sich auf die veraltete und unsichere WEP-Verschlüsselung verlassen.
- Deaktivieren Sie die SSID-Aussendung (Service Set Identifier), um die Präsenz Ihres drahtlosen Geräts nicht öffentlich zu machen.
- Ändern Sie den standardmäßigen SSID-Namen Ihres Geräts. Für einen Hacker ist es nicht schwer, den standardmäßigen Namen des Herstellers herauszufinden und damit Ihr drahtloses Netzwerk zu orten. Vermeiden Sie Namen, die sich einfach erraten lassen, und folgen Sie bei der Wahl des Namens den Richtlinien im hinteren Teil dieses Ratgebers..
- Achten Sie beim Kauf eines Routers darauf, dass dieser NAT (Network Address Translation) unterstützt. Damit ist Ihr Computer für externe Angreifer unsichtbar; sie können nur den Router selbst erkennen.

So schützen Sie Ihr drahtloses Netzwerk:

✓ Ändern Sie das Administratorkennwort.

✓ Aktivieren Sie die Verschlüsselung.

✓ Deaktivieren Sie SSID, und ändern Sie den standardmäßigen Namen Ihres drahtlosen Routers.

✓ Beachten Sie die Hinweise zum Schutz vor bösartigem Code und Hacker-Angriffen.

Was bedeutet Spam?

Spam sind anonyme, unerwünschte Massen-E-Mails, das elektronische Gegenstück zu unerwünschten Postwurfsendungen. Bei ca. 70–80 % aller gesendeten E-Mails handelt es sich um Spam.

Spam wird versendet, um für Produkte und Services zu werben. Spammer versenden große Mengen an E-Mails und verdienen ihr Geld durch den Verkauf von Produkten an diejenigen, die darauf reagieren. In der Regel reagiert nur ein sehr kleiner Prozentsatz auf solche E-Mails; doch dies reicht den Spammern bereits aus, um Profit zu machen.

Es ist zeitraubend und ärgerlich, sich durch Massen von Spam-Mails (auch Junk-Mails genannt) durchzukämpfen. Zudem werden Ihr Posteingang überfüllt und unnötig Bandbreite und Speicherplatz verbraucht. Außerdem sollte ein weiterer wichtiger Punkt berücksichtigt werden: Spam-E-Mails können bösartige Programme enthalten. Ihr Anhang kann infiziert sein, oder sie können einen Link zu einer Website mit einem bösartigen Programm enthalten (dieser Code kann beim Besuch der Website automatisch heruntergeladen und auf Ihrem Computer installiert werden, wenn Sie nicht mit Sicherheitspatches vorgesorgt haben).

Spammer nutzen **Botnetze**, um ihre E-Mails zu verbreiten. Botnetze sind Netzwerke von Computern, die mithilfe von Trojanern oder anderem bösartigen Code von Cyberkriminellen übernommen wurden. Das Opfer bemerkt nicht, dass die Spammer seinen Computer fernsteuern können, doch über die infizierten Rechner werden automatisch Junk-Mails an andere Personen gesendet. Schützen Sie Ihren Computer daher mit Internet-Sicherheitssoftware, um das Risiko einer solchen Übernahme zu minimieren.

Durch Spam-E-Mails verlieren Sie kostbare Zeit, Ihr Posteingang quillt über, und es werden unnötig Bandbreite und Speicherplatz verbraucht; außerdem kann durch sie bösartiger Code verbreitet werden.

Dennis ist geschützt.

Dennis kann sich ein Leben ohne Internet gar nicht vorstellen. Er trifft Freunde in Web-Communities, kauft in Online-Shops und verbringt viel Zeit auf seinen Lieblings-Webseiten sowie in virtuellen Welten. Wegen Cybercrime macht er sich keine Sorgen, auch wenn Kriminelle im Internet täglich mit über 17.000 neuen Bedrohungen auf seine persönlichen Daten und Passwörter aus sind. Online-Betrug, Identitätsdiebstahl und das Ausspionieren von Passwörtern – all das bereitet Dennis keine schlaflosen Nächte.

Wie kann ich mich vor Spam schützen?

Beachten Sie die Hinweise zu Ihrem Schutz vor bösartigem Code und Hacker-Angriffen. Zusätzlich können Sie durch Beachtung der folgenden Regeln die Menge an Spam, die Sie erhalten, erheblich reduzieren.

- Antworten Sie nicht auf Spam-E-Mails. Oft verifizieren Spammer den Empfang und protokollieren die Antworten, so dass Sie durch eine Antwort das Risiko nur erhöhen, in Zukunft noch mehr Spam zu erhalten.
- Klicken Sie in Spam-E-Mails nicht auf Links zum Abbestellen. Dadurch bestätigen Sie, dass Ihre E-Mail-Adresse aktiv ist, und Sie werden weiterhin von Spammern belästigt.
- Verwenden Sie mehrere E-Mail-Adressen. Nutzen Sie eine für die persönliche Korrespondenz und mindestens eine weitere für öffentliche Foren, **Chat-Räume**, Mailing-Listen und andere öffentliche Websites oder Services. Falls Sie dann irgendwann zu viele Spam-E-Mails erhalten sollten, können Sie Ihre öffentliche Adresse einfach löschen und eine neue erstellen.
- Erstellen Sie eine schwer zu erratende private E-Mail-Adresse. Spammer kombinieren bei der Zusammensetzung möglicher Adressen offensichtliche Namen, Wörter und Zahlen. Seien Sie also kreativ, und verwenden Sie nicht nur Ihren Vor- und Nachnamen.
- Geben Sie Ihre private Adresse nirgends öffentlich bekannt. Wenn Sie keine Wahl haben, tarnen Sie die Adresse, so dass sie von den automatisierten Tools nicht erkannt wird, mit denen Spammer E-Mail-Adressen im Internet sammeln. Schreiben Sie z. B. „paul-punkt-schmidt-at-meinedomain-punkt-com“ anstatt „paul.schmidt@meinedomain.com“.

So können Sie die Menge an Spam, die Sie erhalten, reduzieren:

- ✓ **Antworten Sie nicht auf Spam-E-Mails.**
- ✓ **Klicken Sie in Spam-E-Mails nicht auf Links zum Abbestellen.**
- ✓ **Verwenden Sie mehrere E-Mail-Adressen: eine für den privaten und eine für den öffentlichen Gebrauch.**
- ✓ **Geben Sie Ihre private E-Mail-Adresse nicht öffentlich bekannt, und wählen Sie diese so, dass Sie für Spammer schwer zu erraten ist.**
- ✓ **Beachten Sie die Hinweise zum Schutz vor bösartigem Code und Hacker-Angriffen.**

Warum sind Kennwörter wichtig?

Eine wichtige Methode zum Schutz von vertraulichen Informationen ist die Verwendung eines Kennworts, um den Zugriff anderer Personen auf Ihre persönlichen Daten zu verhindern.

Dies wird heutzutage angesichts der zunehmenden Nutzung des Internets immer wichtiger. Es gibt heute mehr Internetnutzer als je zuvor, und auch Internet-Aktivitäten wie Online-Banking, Online-Shopping und Online-Recherche werden immer vielfältiger. Außerdem wird das Internet verstärkt zum Aufbau sozialer Netzwerke genutzt. In den letzten Jahren ist die Zahl der Social-Networking-Websites wie Facebook, MySpace usw. enorm angestiegen; sie bieten ihren Nutzern die Möglichkeit, beliebige personenbezogene Details sowie Musik-, Bild- und Videodateien auszutauschen.

Doch je mehr persönliche Daten Sie im Internet preisgeben, desto größer auch die Gefahr, Opfer eines **Identitätsdiebstahls** zu werden. Darunter versteht man das Stehlen vertraulicher, personenbezogener Daten durch Kriminelle, die damit Produkte und Dienstleistungen betrügerisch in Ihrem Namen erwerben können. Cyberkriminelle können beispielsweise ein Bankkonto eröffnen oder eine Kreditkarte, einen Führerschein oder einen Reisepass beantragen. Oder sie entwenden einfach Geld direkt von Ihrem Bankkonto.

Kennwörter schützen solch wertvolle Daten und sind daher unverzichtbar. Schützen Sie jedes Ihrer Online-Konten mit einem einmaligen Kennwort, und wählen Sie das Kennwort sorgfältig aus.

Mit Kennwörtern können Sie sich vor Identitätsdiebstahl schützen. Sie erschweren es Cyberkriminellen, Ihre Profildaten zu erfassen, auf Ihr Bankkonto (oder andere Online-Konten) zuzugreifen und Ihr Geld zu stehlen.

Erika ist geschützt.

Erika hält per E-Mail Kontakt zu ihren Enkelkindern, sie kauft gerne online ein und surft im Internet. Wegen Cybercrime macht sie sich keine Sorgen, auch wenn Kriminelle im Internet täglich mit über 17.000 neuen Bedrohungen auf ihr Erspartes aus sind. Online-Betrug, Identitätsdiebstahl oder das Ausspionieren von Passwörtern – all das bereitet Erika keine schlaflosen Nächte.

Ist es wichtig, was ich für ein Kennwort verwende?

Ja, sehr wichtig. Wenn Sie ein ungeeignetes Kennwort verwenden, erhöht sich die Gefahr, Opfer von Cyberkriminalität zu werden. Beachten Sie die Hinweise zu Ihrem Schutz vor bösartigem Code und Hacker-Angriffen. Die nachfolgenden Richtlinien helfen Ihnen bei der Auswahl eines Kennworts für ein Online-Konto.

- Verwenden Sie Kennwörter, die Sie sich gut einprägen können, damit Sie diese nicht aufschreiben oder in einer Datei auf Ihrem Computer speichern müssen (diese Datei könnte von Cyberkriminellen gestohlen werden).
- Verraten Sie niemandem Ihr Kennwort. Falls Sie, zum Beispiel auch telefonisch, aufgefordert werden, Ihr Kennwort preiszugeben, geben Sie keinesfalls personenbezogene Details heraus. Denken Sie immer daran, dass Sie nicht wissen, wer am anderen Ende der Leitung ist.
- Falls Sie von einem Online-Händler oder einer anderen Website eine Bestätigungs-E-Mail mit einem neuen Kennwort erhalten, melden Sie sich bei der Website an und ändern Sie unverzüglich Ihr Kennwort.
- Verwenden Sie keine offensichtlichen Kennwörter, die einfach zu erraten sind, beispielsweise den Namen Ihres Partners, Ihrer Kinder, Ihrer Haustiere, Ihr Fahrzeugkennzeichen, Ihre Postleitzahl usw.
- Verwenden Sie keine echten Wörter, die ein Hacker oder Cyberkrimineller in einem Wörterbuch finden kann.
- Verwenden Sie eine Mischung aus Groß- und Kleinbuchstaben, Zahlen und Sonderzeichen wie Satzzeichen.
- Verwenden Sie falls möglich eine Passphrase anstelle eines einzelnen Worts.
- Verwenden Sie ein Kennwort nicht für mehrere Konten. Findet ein Cyberkrimineller das Kennwort für ein Konto heraus, kann er mit diesem auf weitere Konten zugreifen.
- „Recyceln“ Sie Kennwörter nicht, d. h. verwenden Sie nicht „Kennwort1“, „Kennwort2“, „Kennwort3“ usw. für verschiedene Konten.
- Sorgen Sie dafür, dass Ihre Internet-Sicherheitssoftware Versuche von Cyberkriminellen blockiert, die Kennwörter abfangen oder stehlen möchten.

Der richtige Umgang mit Kennwörtern:

✓ Wählen Sie Kennwörter, die Sie sich gut einprägen können.

✓ Halten Sie diese geheim.

✓ Geben Sie Ihre Kennwörter keinesfalls weiter, selbst wenn eine Berechtigung vorzuliegen scheint.

✓ Verwenden Sie eine Mischung aus Groß- und Kleinbuchstaben, Zahlen und Sonderzeichen.

✓ Verwenden Sie ein Kennwort nicht für mehrere Konten.

✓ „Recyceln“ Sie Kennwörter nicht („Kennwort1“, „Kennwort2“ usw.).

✓ Beachten Sie die Hinweise zum Schutz vor bösartigem Code und Hacker-Angriffen.

Wie kann ich meine Kinder beim sicheren Surfen unterstützen?

Denken Sie zuerst über mögliche Gefahren nach wie beispielsweise:

1. So genannte „**Drive-by-Downloads**“ (d. h. bösartige Programme, die sich beim Besuch einer Website automatisch auf Ihrem Computer installieren).
2. Die Gefahr einer Infektion durch **Peer-to-Peer** (P2P) Filesharing-Software, die anderen Personen Zugriff auf Ihren Computer gewährt.
3. Unerwünschte Werbung einschließlich Pop-ups und **Adware**-Programmen. Diese werden oft automatisch zusammen mit Freeware-Programmen installiert, die über das Internet heruntergeladen werden können.
4. Nicht jugendfreie oder anderweitig anstößige Inhalte.
5. Kinder können von Betrügern zur Herausgabe personenbezogener Informationen (über sich oder über Sie) überredet werden.
6. Kinder laden unter Umständen raubkopiertes Material (z. B. Musik- oder Videodateien) herunter.
7. Kinder können Opfer von Online-Mobbing werden.
8. Kinder können beispielsweise in Chat-Räumen von Pädophilen angesprochen werden.

Kinder sind online genauso angreifbar wie in der wirklichen Welt, und es ist wichtig, dass sie die möglichen Gefahren kennen.

Sie können das Risiko der Gefährdung mithilfe folgender Hinweise einschränken:

- Sprechen Sie mit Ihren Kindern über mögliche Online-Gefahren.
- Platzieren Sie den Computer falls möglich im Wohnzimmer und versuchen Sie, die Nutzung zu einem gemeinsamen Erlebnis für die Familie zu machen.
- Ermuntern Sie Ihre Kinder dazu, mit Ihnen über Online-Erfahrungen zu sprechen, die sie beunruhigen oder ihnen unbehaglich sind.
- Legen Sie Richtlinien fest, was die Kinder dürfen und was nicht. Nachfolgend sind einige Punkte aufgeführt, die Sie bedenken sollten (beachten Sie dabei, dass sich die Antworten mit dem Alter Ihrer Kinder ändern können):
  - Ist die Anmeldung bei sozialen Netzwerken oder anderen Websites in Ordnung?
  - Sind Online-Einkäufe in Ordnung?
  - Ist die Nutzung von **Instant Messaging**-Programmen in Ordnung? Falls Sie diese Frage mit „Ja“ beantworten, sollten Sie Ihren Kindern vermitteln, dass sie nicht mit Unbekannten chatten dürfen.
  - Ist der Besuch von Chat-Räumen in Ordnung?
  - Ist das Herunterladen von Musik-, Video- oder Programmdateien in Ordnung?
- Schränken Sie die Inhalte ein, die mit dem Computer aufgerufen werden können. Viele Internet-Sicherheitslösungen bieten diese Möglichkeit. Zudem enthält der Internet Explorer zu Ihrer Unterstützung einen Inhaltsratgeber. Sie finden ihn unter Extras | Internetoptionen | Inhalte.
- Befolgen Sie die Richtlinien oben, um Ihren Computer vor bösartigen Programmen und Hackern zu schützen, und erklären Sie Ihren Kindern, wie sie dadurch geschützt werden.

So schützen Sie Ihre Kinder online:

✓ Sprechen Sie mit ihnen über mögliche Gefahren.
✓ Stellen Sie den Computer im Wohnzimmer auf.
✓ Ermuntern Sie Ihre Kinder, über ihre Online-Erfahrungen zu sprechen.
✓ Stellen Sie Richtlinien für Online-Aktivitäten auf.
✓ Schränken Sie die Inhalte ein, auf die Ihr Kind online zugreifen kann.
✓ Beachten Sie die Hinweise zum Schutz vor bösartigem Code und Hacker-Angriffen.

Julia ist geschützt.

Julia chattet mit Freunden und surft im Internet. Ihre Eltern wissen trotz der täglich über 17.000 neuen Bedrohungen, dass ihre Familie vor Online-Betrug, Identitätsdiebstahl und dem Abgreifen von Passwörtern geschützt ist.

Dank Kindersicherung kann Julia das Internet gefahrlos nutzen.

Was soll ich tun, wenn mein Computer infiziert ist?

Es ist nicht immer einfach festzustellen, ob ein Computer infiziert ist. Die Urheber von Viren, Würmern, Trojanern und Spyware unternehmen immer größere Anstrengungen, ihren Code zu verstecken und den auf einem infizierten Computer angerichteten Schaden zu verschleiern. Deshalb ist es so wichtig, dass Sie die Hinweise in diesem Ratgeber beachten. Insbesondere sollten Sie Internet-Sicherheitssoftware installieren, regelmäßig Ihr Betriebssystem und Ihre Anwendungen aktualisieren und Ihre Daten regelmäßig sichern.

Es ist äußerst schwierig, eine Liste mit charakteristischen Symptomen eines infizierten Computers zu erstellen, da die selben Symptome auch bei Hardware- und/oder Softwareproblemen auftreten können. Nachfolgend finden Sie einige Beispiele:

- Ihr Computer verhält sich ungewöhnlich, d. h. anders als bislang.
- Es werden unerwartete Mitteilungen oder Bilder angezeigt.
- Sie hören zufällige und unerwartete Audiosignale.
- Programme werden unerwartet gestartet.
- Ihre Firewall weist Sie darauf hin, dass eine Anwendung (die Sie nicht gestartet haben) eine Verbindung mit dem Internet herstellen möchte.
- Ihre Bekannten weisen Sie darauf hin, dass Sie E-Mails von Ihrer Adresse erhalten haben, die Sie nicht geschickt haben.
- Ihr Computer hängt häufig, oder Programme laufen langsamer.
- Sie erhalten viele System-Fehlermeldungen.
- Das Betriebssystem wird beim Starten des Computers nicht geladen.
- Sie stellen fest, dass Dateien oder Ordner gelöscht oder geändert wurden.
- Sie stellen Festplattenaktivität fest, obwohl keine Programme ausgeführt werden.
- Ihr Webbrowser verhält sich unberechenbar, Sie können beispielsweise ein Browserfenster nicht schließen.

Keine Panik, falls eines dieser Symptome auftritt. Sie haben vielleicht ein Hardware- oder Softwareproblem, und der Computer ist nicht von einem Virus, Wurm oder Trojaner infiziert. Sie sollten Folgendes unternehmen:

- Trennen Sie die Verbindung Ihres Computers mit dem Internet.
- Falls Ihr Computer mit einem LAN verbunden ist, trennen Sie ihn vom Netzwerk.
- Falls Ihr Betriebsystem nicht startet, starten Sie den Computer im abgesicherten Modus (halten Sie beim Einschalten des Computers die Taste F8 gedrückt und wählen Sie im angezeigten Menü „Abgesicherter Modus“), oder starten Sie den Computer von einer Rettungs-CD.
- Falls Sie nicht über eine aktuelle Datensicherung verfügen, sichern Sie Ihre Daten.
- Stellen Sie sicher, dass Ihre Antiviren-Datenbanken auf dem aktuellsten Stand sind. Falls möglich, laden Sie die Updates nicht mit dem möglicherweise infizierten Computer herunter, sondern verwenden Sie einen anderen Computer, z. B. den eines Bekannten. Wichtig: Falls Ihr Computer infiziert ist und Sie eine Verbindung mit dem Internet herstellen, kann ein bösartiges Programm wichtige Daten an einen entfernten Hacker senden oder sich selbst an Personen verschicken, deren E-Mail-Adressen auf Ihrem Computer gespeichert sind.
- Scannen Sie den gesamten Computer.

- Wird ein bösartiges Programm gefunden, befolgen Sie die Richtlinien des Herstellers Ihrer Internet-Sicherheitssoftware. Hochwertige Sicherheitssoftware bietet Optionen zur Desinfektion infizierter Objekte, eine Quarantäne für Objekte, die unter Umständen infiziert sind, und löscht Würmer und Trojaner. Sie erstellt zudem eine Berichtsdatei mit einer Liste aller infizierten Dateien und bösartigen Programme, die auf dem Computer gefunden wurden.
- Falls Ihre Internet-Sicherheitssoftware nichts findet, ist Ihr Computer wahrscheinlich nicht infiziert. Überprüfen Sie die Hardware und die auf dem Computer installierte Software (entfernen Sie nicht lizenzierte Software und nicht erforderliche Dateien), und prüfen Sie, ob Sie über die aktuellsten Updates für Ihr Betriebssystem und Ihre Anwendungen verfügen.
- Falls beim Entfernen bösartiger Programme Probleme auftreten, suchen Sie auf der Website des Herstellers Ihrer Internet-Sicherheitssoftware nach Informationen zu speziellen Hilfsprogrammen, die für das Entfernen eines bestimmten bösartigen Programms unter Umständen erforderlich sind.
- Wenden Sie sich falls erforderlich an den technischen Support des Herstellers Ihrer Internet-Sicherheitssoftware für weitere Unterstützung. Dort erfahren Sie auch, wie Sie eine Beispieldatei zur Untersuchung durch einen Virenforscher einreichen können.

Falls Ihr Computer unter Umständen infiziert ist:

✓ Keine Panik!

✓ Trennen Sie die Verbindung Ihres Computers mit dem Internet.

✓ Sichern Sie Ihre Daten.

✓ Aktualisieren Sie Ihre Antiviren-Datenbanken.

✓ Scannen Sie Ihren Computer.

✓ Wird nichts gefunden, überprüfen Sie Ihren Computer auf Hardware- oder Softwareprobleme.

✓ Sollten weiterhin Probleme auftreten, wenden Sie sich an den Hersteller Ihrer Internet-Sicherheitssoftware.

Abschließende Bemerkung zu Identitätsdiebstahl

Denken Sie daran, dass Offline-Sicherheit ebenso wichtig ist. Physische Daten können von Identitätsdieben für den Zugriff auf Ihre Online-Konten verwendet werden. Investieren Sie in einen Aktenvernichter (am besten mit Querschnitt), und zerstören Sie alle Dokumente mit personenbezogenen Daten (Name, Adresse, Geburtsdatum usw.) vor der Entsorgung.

Kaufen Sie einen Aktenvernichter mit Querschnitt, und zerstören Sie alle Dokumente mit personenbezogenen Daten vor der Entsorgung.

Nützliche Webseiten

www.stop-cybercrime.de
www.kaspersky.de
www.viruslist.de

Ein umfangreiches Glossar der in diesem Ratgeber verwendeten Begriffe finden Sie online unter www.stop-cybercrime.de/glossar.