

# Alles sicher?

*Dieser Text handelt von Sicherheitsrisiken, die bei der allzu sorglosen Nutzung von Mobiltelefonen lauern können. Ärgerlicherweise hat sich offensichtlich ein Virus eingeschlichen und sein Unwesen getrieben. Kannst du den Beschreibungen der Risiken die richtigen Bezeichnungen zuordnen?*

Apps

Schadsoftware

Bluetooth- und Infrarotschnittstellen

W-LAN-Netze

Dank der Weiterentwicklung der Mobiltelefone ist unser Leben um vieles leichter und amüsanter geworden. Mit einem Handy können wir heute noch viel mehr als nur telefonieren!

Dieses Mehr an Nutzungsmöglichkeiten hat leider auch zu einem Mehr an Sicherheitsrisiken geführt. Wer diese allerdings kennt und weiß, wie er sich und seine Daten vor Missbrauch schützen kann, kann die Funktionalitäten moderner Mobiltelefone in vollem Umfang für sich nutzen.

Eine mögliche Sicherheitslücke sind .....

Sie ermöglichen nicht nur den einfachen Austausch von Daten, sondern sind auch eine Eingangstür zu deinem Handy. Achtest du nicht darauf, diese Tür auch wieder zu schließen, nachdem deine erwarteten Gäste eingetrudelt sind, kann es dir schnell passieren, dass plötzlich unerwünschte Eindringlinge mitten in deiner Wohnung stehen – also einfach auf dein Handy zugreifen. Und das ohne dass du es gleich bemerkst. Offene Türen knarren bekanntermaßen nicht …

Aber auch freie ..... können gefährlich sein. Du kannst mit ihrer Hilfe zwar kostenlos surfen, findige Kriminelle, die technisch ein bisschen versiert sind, können dadurch allerdings auch alles mitverfolgen, was du im Internet so „treibst". Daher solltest du, wenn du diese kostenlose Möglichkeit nutzt, um ins Internet einzusteigen, mit Passwörtern, Onlineeinkäufen oder Bankgeschäften lieber doppelt vorsichtig sein. Sonst kann dich das kostenlose Web teuer zu stehen kommen.

Smartphones sind auf dem Vormarsch. Immer mehr Kunden entscheiden sich für eines der neuen klugen Handys, die in vielen Bereichen schon den PC oder Laptop ersetzen. Damit wird diese „Zielgruppe" auch für Programmierer interessant, die sich der Produktion von so genannter..... verschrieben haben.

Es gibt zwar noch relativ wenig bekannte Viren, Würmer und Trojaner, die Handys angreifen, aber Experten rechnen damit, dass diese Zahl in den nächsten Jahren deutlich steigen wird. Ganz nach dem Motto: „Je größer der Markt, umso vielfältiger das Angebot!"

Zu guter Letzt muss man auch die viel gerühmten und beliebten ..... als Sicherheitsrisiko bedenken. Du hast Zeit für ein kurzes Spiel zwischendurch, suchst die nächste Öffi-Haltestelle, oder brauchst kurz einmal eine Wasserwaage? Alles kein Problem! Diese kleinen Programme bieten heute beinahe für jede Frage eine mobile Lösung. Wer allerdings bei der Installation der Miniprogramme allzu sorglos vorgeht, dem kann es passieren, dass er sich damit einen Spion ins Handy setzt. Denn manche Programme greifen auf Bereiche des Telefons zu, in denen sie eigentlich nichts verloren haben, und übermitteln Daten an den Programmhersteller, die privat sind und auch privat bleiben sollten.



# Alles sicher?

*Dieser Text handelt von Sicherheitsrisiken, die bei der allzu sorglosen Nutzung von Mobiltelefonen lauern können. Ärgerlicherweise haben sich offensichtlich einige Viren eingeschlichen und ihr Unwesen getrieben. Kannst du den Beschreibungen der Risiken die richtigen Bezeichnungen zuordnen? Außerdem gilt es, die richtige s-Schreibung zu ergänzen!*

**Apps**

**Bluetooth- und Infrarotschnittstellen**

**W-LAN-Netze**

**Schadsoftware**

Dank der Weiterentwicklung der Mobiltelefone ist unser Leben um vieles leichter und amü ..... anter geworden. Mit einem Handy können wir heute noch viel mehr als nur telefonieren!

Dieses Mehr an Nutzungsmöglichkeiten hat leider auch zu einem Mehr an Sicherheitsri ..... iken geführt. Wer diese allerdings kennt und wei ..... , wie er sich und seine Daten vor Mi ..... brauch schützen kann, kann die Funktionalitäten moderner Mobiltelefone in vollem Umfang für sich nutzen.

Eine mögliche Sicherheitslücke sind .....

Sie ermöglichen nicht nur den einfachen Austausch von Daten, sondern sind auch eine Eingangstür zu deinem Handy. Achtest du nicht darauf, die ..... e Tür auch wieder zu schlie ..... en, nachdem deine erwarteten Gäste eingetrudelt sind, kann es dir schnell pa ..... ieren, da ..... plötzlich unerwünschte Eindringlinge mitten in deiner Wohnung stehen – also einfach auf dein Handy zugreifen. Und da ..... ohne da ..... du es gleich bemerkst. Offene Türen knarren bekannterma ..... en nicht …

Aber auch freie ..... können gefährlich sein. Du kannst mit ihrer Hilfe zwar kostenlos surfen, findige Kriminelle, die technisch ein bi ..... chen ver ..... iert sind, können dadurch allerdings auch alles mitverfolgen, was du im Internet so „treibst". Daher solltest du, wenn du diese ko ..... tenlose Möglichkeit nutzt, um ins Internet einzusteigen, mit Pa ..... wörtern, Onlineeinkäufen oder Bankgeschäften lieber doppelt vorsichtig sein. Son ..... t kann dich das ko ..... tenlose Web teuer zu stehen kommen.



Smartphones sind auf dem Vormarsch. Immer mehr Kunden entscheiden sich für eines der neuen klugen Handys, die in vielen Bereichen schon den PC oder Laptop ersetzen. Damit wird diese „Zielgruppe“ auch für Programmierer intere ..... ant, die sich der Produktion von so genannter ..... verschrieben haben.

Es gibt zwar noch relativ wenig bekannte Viren, Würmer und Trojaner, die Handys angreifen, aber Experten rechnen damit, dass diese Zahl in den nächsten Jahren deutlich steigen wird. Ganz nach dem Motto: „Je grö ..... er der Markt, um ..... o vielfältiger das Angebot!“

Zu guter Letzt mu ..... man auch die viel gerühmten und beliebten ..... als Sicherheitsrisiko bedenken.

Du ha ..... t Zeit für ein kurzes Spiel zwischendurch, suchst die nächste Öffi-Haltestelle, brauchst kurz einmal eine Wa ..... erwaage oder möchtest, bevor du zur Ka ..... e gehst, noch rasch einen aktuellen Preisvergleich durchführen? Alles kein Problem! Diese kleinen Programme bieten heute beinahe für jede Frage eine mobile Lösung!

Wer allerdings bei der In ..... tallation der Miniprogramme allzu sorglos vorgeht, dem kann es pa ..... ieren, da ..... er sich damit selbst einen Spion ins Handy setzt. Denn manche Programme greifen auf Bereiche des Telefons zu, in denen sie eigentlich nichts verloren haben, und übermitteln Daten an den Programmhersteller, die privat sind und auch privat bleiben sollten.



**Verständnisfragen zum Text „Alles sicher?“**

*Welche Funktionen bieten moderne Handys? Wofür kann man sie nutzen?*

.....

.....

.....

.....

*Wofür werden Bluetooth- und Infrarotschnittstellen beim Handy genutzt?*

.....

.....

*Hast du schon einmal eine dieser Schnittstellen genutzt? Wenn ja – wofür?*

.....

.....

*Welche Möglichkeit bieten freie W-LAN-Netze?*

.....

.....

*Hast du schon einmal ein freies W-LAN-Netz genutzt?*

❒ Ja ❒ Nein

*Worauf sollte man bei der Nutzung freier W-LAN-Netze achten?*

.....

.....

*Welche Bedrohungen kann man unter dem Überbegriff „Schadsoftware“ zusammenfassen?*

.....

.....

*Was solltest du bei der Installation von Apps bedenken?*

.....

.....





# Alles sicher?

Dank der Weiterentwicklung der Mobiltelefone ist unser Leben um vieles leichter und amüsanter geworden. Mit einem Handy können wir heute noch viel mehr als nur telefonieren! Dieses Mehr an Nutzungsmöglichkeiten hat leider auch zu einem Mehr an Sicherheitsrisiken geführt. Wer diese allerdings kennt und weiß, wie er sich und seine Daten vor Missbrauch schützen kann, kann die Funktionalitäten moderner Mobiltelefone in vollem Umfang für sich nutzen.

Eine mögliche Sicherheitslücke sind **Bluetooth- und Infrarotschnittstellen**. Sie ermöglichen nicht nur den einfachen Austausch von Daten, sondern sind auch eine Eingangstür zu deinem Handy. Achtest du nicht darauf, diese Tür auch wieder zu schließen, nachdem deine erwarteten Gäste eingetrudelt sind, kann es dir schnell passieren, dass plötzlich unerwünschte Eindringlinge mitten in deiner Wohnung stehen – also einfach auf dein Handy zugreifen. Und das ohne dass du es gleich bemerkst. Offene Türen knarren bekanntermaßen nicht …

Aber auch freie **W-LAN-Netze** können gefährlich sein. Du kannst mit ihrer Hilfe zwar kostenlos surfen, findige Kriminelle, die technisch ein bisschen versiert sind, können allerdings auch alles mitverfolgen, was du im Internet so „treibst". Daher solltest du, wenn du diese kostenlose Möglichkeit nutzt, um ins Internet einzusteigen, mit Passwörtern, Onlineeinkäufen oder Bankgeschäften lieber doppelt vorsichtig sein. Sonst kann dich das kostenlose Web teuer zu stehen kommen.

Smartphones sind auf dem Vormarsch. Immer mehr Kunden entscheiden sich für eines der neuen klugen Handys, die in vielen Bereichen schon den PC oder Laptop ersetzen. Damit wird diese „Zielgruppe" auch für Programmierer interessant, die sich der Produktion von so genannter **Schadsoftware** verschrieben haben. Es gibt zwar noch relativ wenig bekannte Viren, Würmer und Trojaner, die Handys angreifen, aber Experten rechnen damit, dass diese Zahl in den nächsten Jahren deutlich steigen wird. Ganz nach dem Motto: „Je größer der Markt, umso vielfältiger das Angebot!"

Zu guter Letzt muss man auch die viel gerühmten und beliebten **Apps** als Sicherheitsrisiko bedenken. Du hast Zeit für ein kurzes Spiel zwischendurch, suchst die nächste Öffi-Haltestelle, brauchst kurz einmal eine Wasserwaage oder möchtest, bevor du zur Kasse gehst, noch rasch einen aktuellen Preisvergleich durchführen? Alles kein Problem! Diese kleinen Programme bieten heute beinahe für jede Frage eine mobile Lösung. Wer allerdings bei der Installation der Miniprogramme allzu sorglos vorgeht, dem kann es passieren, dass er sich damit selbst einen Spion ins Handy setzt. Denn manche Programme greifen auf Bereiche des Telefons zu, in denen sie eigentlich nichts verloren haben, und übermitteln Daten an den Programmhersteller, die privat sind und auch privat bleiben sollten.



# All safe?

*This text is about security risks that may lure when mobile phones are used too carelessly. Unfortunately a virus has sneaked in and has caused some chaos. Can you match the correct terms with the descriptions of risks?*

apps

malware

Bluetooth and infrared interfaces

wifi networks

Thanks to the development of mobile phones our life has become far more easier and more amusing. We can do a lot more with a mobile phone than make phone calls! Unfortunately, this increase in possibilities of use has led to an increase in security risks. However, those who are familiar with those risks and know how to protect their data against misuse can use the full range of functionalities of modern mobile phones.

One potential security lapse are ..... . They enable not only an easy exchange of data but also are a door into your mobile phone. If you do not close this door after the guests you expected have arrived it may soon happen that unwanted intruders stand right in the middle of your flat, i.e. access your mobile phone. And this may happen without you knowing it at once. As we know, open doors usually do not creak…

However, free..... can be dangerous. You can use them to surf on the internet for free; however, clever criminals with some technical expertise can follow every step you take on the internet. Therefore you should rather be double careful in using passwords, going online shopping or making your banking transactions if you use this free possibility to access the internet. Otherwise the free web can be rather expensive.

Smartphones are about to take the lead. An increasing number of customers chooses one of the new clever mobile phones which in many areas already replace the PC or notebook. Therefore this „target group" becomes more and more interesting for programmers who dedicate their work to the production of so-called ..... ..... . Although there are still very little known viruses, worms and Trojans that attack mobile phones, experts expect this number to increase significantly in the next years. As the saying goes: „The bigger the market, the greater the variety of offers!"

Finally, one must also consider the highly acclaimed and popular ..... as a security risk. You have got time for a quick game, are looking for the next bus or tram stop, quickly need a water level or want to make a quick price check before you proceed to the cashier's desk? No problem! Nowadays these small programmes offer a mobile solution for almost every question. However, those who act too carelessly when installing those mini programmes might place a little spy into their mobile phone themselves. For some programmes access areas of the phone which actually should be off limits for them and transmit data to the programme manufacturer that are and should continue to be private.



# All safe?

*This text is about security risks that may lure when mobile phones are used too carelessly. Unfortunately a virus has sneaked in and has caused some chaos. Can you match the correct terms with the descriptions of risks and complete the text with the right verbs?*

**apps**

**Bluetooth and infrared interfaces**

**malware**

**wifi networks**

Thanks to the development of mobile phones our life has ..... far more easier and more amusing. We can do a lot more with a mobile phone than make phone calls!

Unfortunately, this increase in possibilities of use has ..... to an increase in security risks. However, those who ..... familiar with those risks and know how to ..... their data against misuse can ..... the full range of functionalities of modern mobile phones.

**are**
**arrived**
**be**
**become**
**chooses**
**close**
**creak**
**dedicate**
**enable**
**follow**
**increase**
**installing**
**led**
**making**
**offer**
**protect**
**transmit**
**use**

One potential security lapse are ..... .

They ..... not only an easy exchange of data but also are a door into your mobile phone. If you do not ..... this door after the guests you expected have ..... it may soon happen that unwanted intruders stand right in the middle of your flat, i.e. access your mobile phone. And this may happen without you knowing it at once. As we know, open doors usually do not ..... .

However, free ..... can be dangerous. You can use them to surf on the internet for free; however, clever criminals with some technical expertise can ..... every step you take on the internet. Therefore you should rather ..... double careful in using passwords, going online shopping or ..... your banking transactions if you use this free possibility to access the internet.

Otherwise the free web can be rather expensive.

# Smart & Safe

FORUM MOBILKOMMUNIKATION

Smartphones are about to take the lead. An increasing number of customers ..... one of the new clever mobile phones which in many areas already replace the PC or notebook. Therefore this „target group“ becomes more and more interesting for programmers who ..... their work to the production of so-called ..... . Although there are still very little known viruses, worms and Trojans that attack mobile phones, experts expect this number to ..... significantly in the next years. As the saying goes: „The bigger the market, the greater the variety of offers!“

Finally, one must also consider the highly acclaimed and popular ..... as a security risk.

You have got time for a quick game, are looking for the next bus or tram stop, quickly need a water level or want to make a quick price check before you proceed to the cashier‘s desk?

No problem! Nowadays these small programmes ..... ..... a mobile solution for almost every question. However, those who act too carelessly when ..... those mini programmes might place a little spy into their mobile phone themselves. For some programmes access areas of the phone which actually should be off limits for them and .....data to the programme manufacturer that are and should continue to be private.



# Lots of verbs ...

*Fill in the correct form of the verb and translate into German!*

| | infinitive | Perfect tense | Past tense | German translation |
|---|---|---|---|---|
| are | be | I have been | I was | sein |
| arrived | | she | she | |
| be | | they | they | |
| become | | you | you | |
| chooses | | he | he | |
| close | | I | I | |
| creak | | it | it | |
| dedicate | | I | I | |
| enable | | you | you | |
| follow | | they | they | |
| increase | | it | it | |
| installing | | I | I | |
| led | | it | it | |
| making | | you | you | |
| offer | | we | we | |
| protect | | she | she | |
| transmit | | you | you | |
| use | | I | I | |



**Questions on understanding**

*What functions do modern mobile phones offer? What can you use them for?*

.....

.....

.....

.....

*What are Bluetooth and infrared interfaces in mobile phones used for?*

.....

.....

*Have you ever used one of those interfaces? If so, what for?*

.....

.....

*What possibilities do free wifi networks offer?*

.....

.....

*Have you ever used a free wifi network?*

❒ Yes ❒ No

*What should be considered when using free wifi networks?*

.....

.....

*What threats can be summarised under the term „malware“?*

.....

.....

*What should you consider when installing an app?*

.....

.....



# Lots of verbs ...

| | infinitive | Perfect tense | Past tense | German translation |
|---|---|---|---|---|
| are | to be | I have been | I was | sein |
| arrived | to arrive | she has arrived | she arrived | ankommen |
| be | to be | they have been | they were | sein |
| become | to become | you have become | you become | werden |
| chooses | to choose | he has chosen | he chose | wählen |
| close | to close | I have closed | I closed | schließen |
| creak | to creak | it has creaked | it creaked | knarren |
| dedicate | to dedicate | I have dedicated | I dedicated | widmen |
| enable | to enable | you have enabled | you enabled | können |
| follow | to follow | they have followed | they followed | folgen |
| increase | to increase | it has increased | it increased | ansteigen |
| installing | to install | I have installed | I installed | installieren |
| led | to lead | it has led | it led | führen |
| making | to make | you have made | you made | machen |
| offer | to offer | we have offered | we offered | anbieten |
| protect | to protect | she has protected | she protected | schützen |
| transmit | to transmit | you have transmitted | you transmitted | übermitteln |
| use | to use | I have used | I used | gebrauchen |



# Schutzschild aktiv?

## Öffentliches WLAN ist Sicherheitsrisiko

Wer mit seinen persönlichen Daten sorglos umgeht, spielt Cyberkriminellen direkt in die Hände. Die wichtigsten Hinweise für die sichere Nutzung öffentlicher Netze.

Mobil ins Internet: Dank öffentlich zugänglichem WLAN ist das besonders einfach möglich. Doch das lockt Kriminelle an.

Mit dem Handy, dem Laptop oder dem Tablet kann heute überall ins Internet eingestiegen werden. Dabei ist öffentlich zugängliches WLAN (ein lokales Funknetz) für diesen Zugang ins Web bei den Nutzern mobiler Geräte äußerst beliebt - schließlich punktet WLAN gegenüber Mobilfunkverbindungen in der Regel mit stabileren Verbindungen. Doch diese Funknetze machen es Kriminellen gleichzeitig deutlich leichter, an sensible Daten wie Kreditkartendetails, E-Mail-Pass¬wörter oder Informationen über das Online-Banking zu kommen, warnt das IT-Security-Unternehmen BullGuard.

### Die wichtigsten Tipps

Eine beliebte Methode der Cyberkriminellen ist dabei das Installieren sogenannter Fake-APs (Access-Points). Fallen Anwender darauf herein, verbinden sie sich mit diesem falschen Netz, anstatt mit dem des bekannten WLAN-Providers. Kriminelle schneiden dann alle übertragenen Daten mit.

Aber auch ohne diesen Trick lassen sich alle Daten einholen, wenn sie unverschlüsselt über ein WLAN wandern. Stellt sich also die Frage, wie man als mobiler Nutzer dieses Risiko verringern kann. Die Security-Experten von Bull Guard geben dazu folgende Tipps für den Schutz gegen möglichen Datenklau:

- Möglichst wenig sensible Daten über das Netz senden, das gilt vor allem für unbekannte Netze.
- Zu empfehlen ist der Einsatz von verschlüsselten Verbindungen: E-Mail-Provider bieten in der Regel an, die Post über eine mit SSL oder TLS verschlüsselte Verbindung abzurufen. VPNs verbergen alle Daten vor neugierigen Blicken.
- Security-Software nutzen: Auch für Android, iPhone und Co. gibt es zahlreiche Schadprogramme (Malware), die man sich im öffentlichen WLAN einfangen kann. Auf jedes Smartphone gehört daher wie bei Laptop und PC eine Security-Lösung mit Antivirensoftware und Firewall.
- WLAN ausschalten: Braucht man kein WLAN, ist es am besten, diese Funktion auf dem Gerät auszuschalten. Dann kann das Smartphone nicht automatisch eine WLAN-Verbindung aufbauen, wenn es in Reichweite eines Hotspots (öffentliches Netz) kommt. Die automatische WLAN-Erkennung und -Verbindung sollte daher ebenfalls ausgeschaltet werden.
- Um Anwender auf ihr eigenes Netz zu locken, wählen Kriminelle für das WLAN einen Namen, der dem des Providers sehr ähnlich ist. Anwender sollten also genau auf den Namen des Funknetzes achten, mit dem sie sich verbinden.

http://wirtschaftsblatt.at/archiv/aktuell/1216217/print.do

## Böse Zwillinge / Evil Twins

Hot-Spots an öffentlichen Plätzen können von Hackern missbraucht werden. Und das könnte so aussehen: Ein Hacker setzt sich in ein Cafe und hat ein Laptop in seinem Rucksack. Dieser Laptop hat eine WLAN-Karte und ist als Access-Point ins Internet eingerichtet. Es kann auch sein, dass er den richtigen Hot-Spot im Cafe durch eine Attacke ausgeschaltet hat und alle Einstellungen auf seinen Laptop übertragen hat. Der Hacker hat nun einen sogenannten bösen Zwilling dabei. Wenn sich ein Besucher des Cafes ins Internet einloggen will, kann es sein, dass er beim bösen Zwilling landet. Der Hacker kann dann alles sehen, was das ahnungslose Opfer im Internet treibt: Er kann fremde E-Mails lesen, Passwörter stehlen und sogar an die wichtigen Daten von Kreditkarten kommen. So ein böser Zwilling kann also nicht nur sehr persönliche Daten ausspionieren, sondern auch richtig teuer werden.

http://www.handysektor.de/index.php/a_bis_z/page/boese_zwillinge_evil_twins

## WLAN-Verbindung auf Smartphones absichern

Die Nutzung von WLAN vom Android-Smartphone aus ist nicht immer sicher. Wir zeigen, wie Sie WLAN-Verbindungen auf Smartphones absichern. Man hat herausgefunden, dass Google für die App-Authentifizierung bei den eigenen Diensten eine digitale Visitenkarte („Authentication Token“) häufig unverschlüsselt zurückgeschickt hat. Wird dieses Token von einem Hacker abgefangen, dann kann er sich bei Google etwa als Sie ausgeben und Ihre dort hinterlegten Daten abgreifen. Die Lücke ist mittlerweile natürlich gestopft, veranschaulicht aber ganz gut das neue Risikopotenzial der ultramobilen Geräte.

Android & iOS Smartphones vor der WLAN-Falle schützen

**SSIDs öffentliche WLANs löschen:** Wenn Sie mit Ihrem Smartphone oder Tablet in einem öffentlichen WLAN surfen, dann ist dessen SSID als bekannt in Ihrem Gerät hinterlegt. Falls Sie nun an einem anderen WLAN vorbeilaufen, das dieselbe SSID (und denselben Schlüssel oder keinen Schlüssel) verwendet, bucht sich Ihr Gerät automatisch dort ein. Das ist eine einfache Methode für Hacker, um Sie auszuspionieren. Löschen Sie deshalb öffentliche WLANs aus Ihrem Gerätespeicher, wenn Sie den Ort verlassen. Bei Android tippen Sie dazu auf „Menü  Drahtlos und Netzwerk  WLAN-Einstellungen“, danach auf das zu löschende Netz und in dem aufklappenden Fenster auf den Eintrag „Vergessen“. Bei iOS tippen Sie auf „Einstellungen  WLAN“, dann rechts auf den Pfeil neben dem zu löschenden Netz und auf „Dieses Netzwerk ignorieren“.

**VPN-App:** Genau wie bei PC oder Notebook kann auch bei Smartphones oder Tablets ein VPN-Dienst genutzt werden, um sicher über eine verschlüsselte Vermittlungsstelle zu surfen. Eine kostenlose Möglichkeit für Android bietet hier auch wieder das Tor-Netzwerk. Laden Sie sich dazu zunächst die kostenlose App Orbot herunter, und installieren Sie sie. Nach dem Sie die App gestartet haben, tippen und halten Sie den großen Knopf in der Mitte, um sich mit dem Tor-Netzwerk zu verbinden. Nun benötigen Sie noch einen Browser, der sich über Orbot und das Tor-Netzwerk mit dem Internet verbindet. Laden Sie dazu den Browser Orweb und installieren und starten Sie ihn. Es öffnet sich eine Seite mit dem Text „Congratulations. Your browser is configured to use Tor“. Tippen Sie auf die Menü-Taste und „Go“, um eine Internetadresse eingeben und sie ansurfen zu können.

Auch hier besteht natürlich das klassische Tor-Problem. Die Verbindung ist zwar geschützt, aber auch langsam. Schnellere VPN-Dienste sind allerdings kostenpflichtig. Ein guter und schneller VPN-Dienst ist beispielsweise Vyprvpn. Der kostet ab 12,49 Euro/Monat und funktioniert mit Bordmitteln von Android, iPhone, iPad, Windows, Mac-OS X und Linux. Um ihn zu nutzen, klicken Sie auf der Internetseite auf „Buy Now“ und füllen das Formular samt Zahlungsdaten aus. Danach bekommen Sie ein Kennwort zugeschickt. Um den gesamten Datenverkehr über den Vyprvpn-Server zu leiten, folgen Sie der Anleitung für Ihr gewünschtes System unter goldenfrog.com/vyprvpn.

www.pcwelt.de/tipps/Jedes-WLAN-sicher-nutzen-WLAN-Verbindung-auf-Smartphones-absichern-4702884.html



## Apps - Zusatzprogramme für das Smartphone

Sie sind seit geraumer Zeit in aller Munde - Apps, kleine Programme, die auf Smartphones installiert werden, um dessen Funktionen zu erweitern. Egal ob Spiele, News oder schlaue Helferprogramme für das alltägliche Leben - die Auswahl ist gigantisch. Kaum eine Aufgabe, die die kleinen Programme nicht lösen können.

Apps sind aus der alltäglichen Nutzung von Smartphones und inzwischen auch Tablet-Computern kaum noch wegzudenken. Die kleinen Programme, als bunte Fensterchen auf dem Touchscreen eines Smartphones zu erkennen, können in vielen Situationen sehr nützlich sein. Ebenso sind Apps ein netter Zeitvertreib: Zahlreiche Spaßprogramme, Gimmicks und Spiele in den stetig wachsenden App Online-Shops sorgen dafür, dass es immer etwas Neues zu entdecken gibt und keine Langeweile mehr aufkommt.

### Was sind Apps?

App ist die englische Kurzform für „application", was in diesem Zusammenhang so viel bedeutet wie Anwendungsprogramm. Spricht man mit Hinblick auf Handys und Tablets von Apps, sind mit dem Begriff kleine Programme gemeint, die direkt auf dem Mobiltelefon oder Tablet-Computer installiert werden können. Apps werden in speziellen, im Betriebssystem des Geräts integrierten Online-Shops angeboten, wie zum Beispiel dem Apple App Store, Googles Android Market oder der Blackberry Appworld.

### App-Urgesteine

Was so modern und zukunftsweisend klingt, gibt es, wenn auch in wesentlich einfacherer Form, schon seit Jahren. Denn Handy-Anwendungen wie der Wecker, der Taschenrechner, die Stoppuhr oder der Kalender sind unter dem Strich nichts anderes als die heutigen Apps. Als jedoch die Programmiersprache Java so weiterentwickelt wurde, dass sie für Mobiltelefone nutzbar wurde, wuchsen auch die Möglichkeiten für Applikationen. Kleine Anwendungen und Spiele konnten über das Internet heruntergeladen und auf dem Telefon installiert werden. Die Möglichkeiten, die diese neue Technik schuf, waren enorm. Es dauerte jedoch bis zum Erscheinen des berühmten iPhones aus dem Hause Apple, welches diese Technik in ihrem vollen Umfang nutzte, bis auch andere Betriebssysteme wie Android nachzogen. So wurden Apps den Mobilfunknutzern in den letzten Jahren in Rekordzeit zugänglich. Inzwischen gibt es in den entsprechenden Online-Shops über 500.000 Apps zum Download.

### Was macht eine App aus?

Im Gegensatz zu normalen Programmen, die erst langwierig installiert werden müssen, ist eine App im Nu geladen und sofort betriebsbereit. Die Auswahl der Apps ist immens. Es gibt simple Werkzeuge und Hilfsprogramme, Spaßanwendungen, Spiele bis hin zu ganzen Programmpaketen mit umfangreichen Funktionen. Die neusten Nachrichten lesen, schnell einen Blick in den Busplan werfen, das Wetter für die nächsten Tage checken, mit einer Übersetzungshilfe nachschauen, was Gutschein auf Französisch heißt, sich schnell ein Taxi zum Aufenthaltsort rufen, Games zocken oder mal eben herausfinden, welches Lied da eben in dem Imbiss lief? Mit Apps ist das alles kein Problem. Ein Fingerzeig auf dem Touchscreen genügt. Auch für Unternehmen lohnt sich inzwischen der Einstieg ins App-Geschäft. Durch die kleinen Programme lassen sich Dienstleistungen via Smartphone in Anspruch nehmen. So beispielsweise die App-Version von Gelbe Seiten. Die Lufthansa-App bietet Fluginformationen für das Mobiltelefon.

Die Kosten für die kleinen Programme variieren. Es gibt Apps für weniger als einen Euro. Zudem sind komplexe Kleinprogramme für an die Tausend Euro verfügbar, so zum Beispiel eine App, durch die man auf Überwachungskamerasysteme zugreifen und diese mit dem iPhone steuern kann. Eine große Anzahl der Programme für das Smartphone sind hingegen auch kostenlos zu haben.

### Die Macht des Apfels

Auch wenn die Erfolgsgeschichte der Apps mit dem Apple iPhone startete, haben sich heute auch andere Handy Betriebssysteme durchgesetzt. Android- und Windows-Smartphones erfreuen sich wachsender Beliebtheit. Die Apps im Apple App Store sind größtenteils kostenpflichtig. Das Angebot des Android Market besteht zu zwei Dritteln aus freien bzw. quelloffenen Programmen. Apple, Google und Microsoft erhalten beim Verkauf einer App 30 Prozent des Kaufpreises als Provision. Der Rest geht an die Entwickler.

Für den Apple App Store gab es in der Vergangenheit jedoch schon heftige Kritik. Der Grund dafür ist die Veröffentlichungspolitik, die Apple mit den Apps im Store betreibt. Denn das Geschäftsmodell gestattet es dem Hersteller, den Einsatz freier Software auf seinen Geräten zu kontrollieren. In der Praxis bedeutet dies,

dass rigoros aussortiert wird, was den Verantwortlichen nicht passt. Dieses Auswahlverfahren unterliegt Kriterien, die nicht offengelegt werden und manchmal als willkürlich erscheinen. So kann es passieren, dass Apps es niemals in den Store schaffen, oder aber im Nachhinein einfach wieder entfernt werden. Apple kann ebenso per Fernzugriff Programme auf dem iPhone löschen, die bereits im App Store gekauft wurden.

**Mehr Auswahl - mehr Risiko**

Im Gegensatz dazu werden Apps von Drittanbietern für das Open Source basierte Android-Betriebssystem im Adroid-Market nicht überprüft. Erst wenn ein User eine App meldet, wird diese geprüft und unter Umständen aus dem Shop entfernt. Auf diese Weise herrscht natürlich große Vielfalt im Adroid-Market. Andererseits besteht so immer die Gefahr, sich schädliche Software herunterzuladen. Derartiger Missbrauch wird durch Apple von Vornherein durch die strikten Kontrollen verhindert.

Doch es gibt weitere Probleme im Adroid-Market: Kritiker dieses App-Modells beäugen nach wie vor kritisch den Datenschutz des Systemkonzepts. Die Sorge besteht darin, Google liefere Kundendaten, die das Unternehmen vermarkten, und mit deren Hilfe ganze Datenprofile der Nutzer erstellt werden können.

**Apps schreiben Erfolgsgeschichte**

Die kleinen Programme sind hilfreich, nützlich oder machen einfach Laune - und es ist wohl auch ihnen zu verdanken, dass von Jahr zu Jahr mehr Smartphones verkauft werden. Zweifelsohne ist die vom Apfel Imperium verfolgte Veröffentlichungspolitik kritisch zu betrachten, aber dennoch lohnt es, sich mit der neuen Technik intensiver auseinanderzusetzen. Eine Alternative ist der Adroid-Market, doch hier ist leider nicht nur die Vielfalt größer, sondern auch das Risiko, sich unerwünschte Software zu installieren, ohne sich dessen bewusst zu sein. Wie bei jedem anderen Software-Programm sollte man also vor der Installation einer App genau schauen, woher diese stammt und ob es sich dabei um eine seriöse, vertrauenswürdige Quelle handelt. Dann steht dem Smartphone-Spaß mit all seinen Facetten nichts mehr im Wege.

www.handytarife.de/index.php?aid=2356

## Wie gehe ich mit Apps sicher um?

- Fragen Sie sich, welche Apps sie w**irklich brauchen** oder unbedingt ausprobieren wollen.
- Lesen Sie die Bewertungen der Apps und in**stallieren sie schlecht bewertete App**s besser **nicht**.
- Löschen Sie Apps, die Sie nicht mehr brauchen. Diese können **im Hintergrund** auch keine **unerwünschten Daten** mehr **übertragen**.
- Installieren Sie nur **Apps aus den offiziellen App-Shops**, da diese entweder vor der Bereitstellung **überprüft** wurden oder bei gröberen Beschwerden aus dem App-Store bzw. vom Handy via Fernlöschung entfernt werden.
- Kontrollieren Sie bei der Installation von Apps die **Zugriffsberechtigungen** (z.B. bei Android-Handys bevor sie auf „Installieren" klicken) und installieren sie eine App, die offensichtlich zu viele Berechtigungen für den Funktionsumfang bietet, lieber nicht.
- Vorsicht mit Apps, die in **sehr reißerischem Stil** oder auffallend schlechtem Deutsch für etwas werben (z.b. für einen „schnellen Gewinn in nur kurzer Zeit", u.ä.). Die Sprache ist oft das beste Warnsignal für betrügerische Apps.
- Nehmen Sie keine **Änderungen am Handybetriebssystem** - **„Jailbreak"** oder **„Rooten"** genannt – vor, da dies die Installation von unsicheren Apps erleichtert und auch die Updates des Handybetriebssystems beeinträchtigen kann.
- Seien Sie besonders bei **kostenlosen Apps und damit verbundenen Werbelinks** vorsichtig. Vorsicht, wenn Kinder mit dem Smartphone spielen. Sie könnten unbemerkt Werbelinks anklicken und **unbewusst Bestellungen tätigen**.
- Sichern Sie Ihr Smartphone gegen unbefugten Zugriff (PIN-Code, **Zugriffsschutz** mit Passwort oder Entsperrmuster) und verwahren Sie es sicher.
- Installieren sie einen **mobilen Virenschutz**, um schädliche Software zu erkennen und löschen zu lassen. Es gibt zahlreiche kostenlose Schutz-Apps von bekannten Anbietern – auch in den App-Shops selbst. Diese ermöglichen u.a. auch eine Ortung Ihres verlorenen Handys, bzw. das Sperren oder Löschen persönlicher Daten.

http://handywissen.at/was-koennen-handys/#c520

## Handy-Viren: erkennen, vermeiden, sich schützen

Handyviren sind immer noch eine Art Mythos. Jeder hat von den fiesen Mobilfunk-Schädlingen gehört. Doch anders als bei Computer-Viren kennen sich die wenigsten Menschen mit ihnen aus, geschweige denn wüssten sie, was genau ein Handyvirus ist, wie man ihn bekommt oder wie man ihm zu Leibe rückt. handytarife.de bringt Licht ins Dunkel.

Bisher sind es wenige Ausnahmen unter den Handy-Usern, die mit Gewissheit von sich behaupten können, dass ihr Mobiltelefon von einem Handyvirus infiziert wurde. Die Wahrscheinlichkeit, sich einen derartigen Schädling einzufangen, ist bis dato überaus gering. Dennoch ist es sehr wahrscheinlich, dass die Zahl der sogenannten Handyviren in Zukunft stark ansteigen wird. Das leuchtet ein, wenn man bedenkt, dass Smartphones sich steigender Beliebtheit erfreuen und bereits heute ein Großteil der Mobilfunknutzer ein internetfähiges Handy benutzt. Eine solche Entwicklung macht diese Handys und ihre Eigentümer natürlich zu einer attraktiven Zielscheibe für Kriminelle. Doch wie kann man sich vor der Gefahr durch Handyviren schützen?

### Virus, Dialer, Wurm oder Trojaner?

Es gibt sowohl Handy-Viren, Handy-Dialer, Handy-Würmer als auch Handy-Trojaner - alle diese Programme gelten als Malware, also schädliche Software.

Handy-Viren sind kleine Programme, die sich auf dem Mobiltelefon einnisten und dann zum Beispiel eigenständig teure Telefonverbindungen herstellen - meistens ohne dass der Handybesitzer es überhaupt bemerkt. Auch teure Premium SMS oder MMS können auf diesem Wege versendet werden. Oft verfügen diese Programme auch über eine Funktion, die es ihnen ermöglicht, sich selbsttätig, beispielsweise über automatischen Selbstversand, weiterzuverbreiten. Ebenso ist es möglich, dass das Handy durch einen Virus, genau wie ein Computer, ausspioniert wird und die kriminellen Hintermänner auf diese Art auf die Jagd nach Bankverbindungen, Passwörtern und anderen wichtigen Daten gehen. Die Handyviren, die bisher entdeckt wurden, griffen übrigens nur Smartphones an.

### Wie verbreitet sich Malware?

Bluetooth, SMS und der Internet-Download sind die gängigsten Wege, sich einen Handyvirus einzufangen. Die schädliche Software kann über alle diese Schnittstellen auf das Handy zugreifen und beliebig Verbindungen aufbauen. Dies passiert meistens, ohne dass es der Eigentümer des Mobiltelefons bemerkt - erst wenn die horrende Rechnung ins Haus flattert, oder sich der Datenmissbrauch auf andere Weise bemerkbar macht, stellt man den Schaden fest.

In den meisten Fällen aktivieren sich die Viren jedoch nicht selbst, sondern es ist in der Tat der Handybesitzer, der sich durch den Virus, verpackt in ein Spiel, ein Bild oder eine sonstige erhaltene Datei, dazu verführen lässt, das Programm unwissentlich zu starten.

Ähnlich wie bei Computern gibt es auch bei den Betriebssystemen, die auf einem Handy installiert sind, Sicherheitslücken und Schwachstellen, die die Hersteller der Schadsoftware gekonnt ausnutzen. Hier sind jedoch vor allem Smartphones betroffen, denn die Kombination aus Mobiltelefon und PDA liefert nicht nur ein leistungsfähiges Betriebssystem, auf dem das Virus sich optimal entfalten kann, sondern bei dieser Art von Mobiltelefon ist die Wahrscheinlichkeit, an sensible Daten wie Passwörter und Kreditkartennummern zu gelangen, am größten.

### Fast immer zu spät bemerkt

Da Handy-Viren bisher bei weitem nicht so erforscht sind und wesentlich seltener auftreten, als die klassischen Computerviren, gibt es leider auch wenige Kennzeichen, die eindeutig auf eine Infektion des Mobiltelefons hinweisen.

Leider stellt man erst viel zu spät fest, dass „fremde Mächte“ auf dem eigenen Handy ihr Unwesen treiben. Wenn die Handyrechnung eine große Anzahl von Anrufen oder SMS an eine unbekannte Nummer aufweist und die Kosten scheinbar grundlos in die Höhe geschossen sind, ist dies jedoch ein ziemlich sicheres Zeichen für einen Dialer- bzw. Virenbefall. Oft haben Betroffene kurze Zeit vorher neue Programme installiert oder MMS von unbekannten Absendern erhalten, geöffnet und damit die schädlichen Programme unwissentlich installiert. Häufig nutzen diese Programme Fehler oder undichte Stellen im Betriebssystem aus.

Aber es muss nicht immer erst die hohe Telefonrechnung ins Haus flattern, bevor man merkt, dass man sich einen Virus eingefangen hat. Denn der Versand

von SMS erfolgt in der Regel durch optische oder akustische Signale, wie Töne oder das Aufleuchten des Handy-Displays. Steht das Handy also nicht mehr still oder leuchtet unentwegt auf, wird man zwangsläufig stutzig.

**Wie man sich vor Handy-Viren schützen kann**
Schneller als man denkt kann sich in so einem Programm, einer Nachricht oder einem harmlos wirkenden Spiel für das Handy ein böses Malware Programm verstecken. Programme, Apps und Anwendungen auf dem Smartphone zu installieren, die nicht aus vertrauenswürdigen Quellen wie den Downloadshops der Handyhersteller stammen, ist immer ein Risiko. Ebenso das Öffnen von fremden Kurz- oder Bildmitteilungen.

Sicherheitslücken im Betriebssystem sind nicht selten das Schlupfloch, durch das die Malware auf das Gerät gelangt. Die Handysoftware auf dem neuesten Stand zu halten und regelmäßig alle wichtigen Updates zu installieren, minimiert also bereits das Risiko, sich Malware einzufangen.

Auch via Bluetooth können Viren, Dialer oder Würmer auf das Handy gelangen. Daher sollte die Bluetooth-Option immer ausgeschaltet sein, wenn sie gerade nicht verwendet wird. Und bitte nicht vergessen, sie nach dem Datentransfer wieder zu deaktivieren.

Wer noch mehr tun möchte, als einfach aufmerksam zu sein und Vorsicht walten zu lassen, kann mit einer Anti-Viren Software für Handys auf Nummer sicher gehen. Hersteller von Virenschutzsoftware für Mobiletelefone sind zum Beispiel F-Secure, Kaspersky oder Symantec. Dialer- oder Einwahlblocker für Handys gibt es bis dato leider noch nicht.

Und wie wird man einen Handyvirus wieder los? Neben dem Virenscanner, der die schädliche Software in Quarantäne setzt, empfiehlt sich ein sogenannter Masterreset, der vom Handynutzer selbst durchgeführt werden kann. Dabei wird das Telefon durch eine bestimmte Tastenkombination, die beim Hersteller erfragt werden kann, wieder auf Werkseinstellung zurückgesetzt. Alle gespeicherten Dateien und Kontakte gehen in der Regel dabei verloren, und auch die Malware wird folglich entfernt. Wer also nicht wie empfohlen seine Daten vom Handy regelmäßig extern sichert, sollte dies vor dem Reset sicherheitshalber tun.

**Fazit: Vorsicht ist besser als Nachsicht**
Mobiltelefone und sogenannte Smartphones erfreuen sind steigender Beliebtheit. Bisher gibt es wenige bekannte Fälle, in denen Handybesitzern großer Schaden durch Handy-Malware zugefügt wurde, und auch die Anzahl der sich im Umlauf befindenden Programme ist bisher noch überschaubar. Dennoch ist zu erwarten, dass sich auf dem Gebiet der Handy-Viren in den kommenden Jahren einiges tun wird - entsprechend ist Vorsicht angesagt. Durch die vielen Schnittstellen, über die der Datentransfer von und auf Smartphones vonstatten gehen kann, entstehen auch diverse Angriffspunkte, die es als Nutzer sorgsam zu schützen gilt. Das funktioniert am besten durch Vorsicht und eine gute Portion gesundes Misstrauen, was Software und Text- sowie Bildnachrichten fremder Absender angeht. Die regelmäßige Installation der vom Hersteller bereitgestellten Software-Updates für das Betriebssystem kann kritische Sicherheitslücken schließen. Auch ein Virenscanner, der nach demselben Prinzip wie die klassischen Virenschutzprogramme auf dem heimischen Rechner funktionieren, bietet zusätzlichen Schutz.

www.handytarife.de/index.php?aid=1929

## Handy-Viren und Handy-Dialer

Handy-Viren und Handy-Dialer haben beste Chancen, die Schädlinge der Zukunft zu werden. Rund 107 Millionen Mobiltelefone sind aktuell in Deutschland angemeldet. Grund genug für Kriminelle, Handys und Smartphones verstärkt ins Visier zu nehmen. Wie Sie sich und Ihr Mobilfunkgerät schützen können, zeigen wir Ihnen in diesem Kapitel.

**Handy-Viren und Handy-Dialer: Was ist das?**
Unter Handy-Dialern versteht man Programme, die sich auf dem Mobiltelefon einnisten und dann hoch tarifierte Verbindungen herstellen. Dabei kann es sich um teure Telefonverbindungen handeln. Ebenso möglich ist aber auch der Versand von hoch tarifierten Premium SMS oder MMS (Multimedia-Kurznachrichten).
Handy-Viren funktionieren ähnlich. Wenn Verbindungsherstellung oder SMS-Versand vom Nutzer unbemerkt und ungewollt vonstatten gehen, handelt es sich um Schadprogramme (Malware), die je nach Ausformung auch als Handytrojaner oder Handyvirus, bzw. Handyviren bezeichnet werden. Enthält das Programm eine Funktion, über die es sich selbst – etwa



über automatischen Selbstversand – weiterverbreiten kann, ist von einem Handy-Wurm die Rede.
Die Grenzen zwischen den verschiedenen Formen von Handy-Schädlingen sind allerdings noch fließend.

**Wie verbreiten sich Handy-Dialer und Handy-Viren?**
Moderne Mobiltelefone haben viele Schnittstellen. Die Folge ist, dass Schadprogramme wie Handy-Viren und Handy-Dialer auch mehr Möglichkeiten haben, sich zu verbreiten. Als Schnittstellen für die Infektion eines Handys können Bluetooth, SMS, aber auch der Download z.B. über eine eingesetzte SIM-Card dienen. In vielen Fällen spielt auch das so genannte Social Engineering eine Rolle: Das Schadprogramm aktiviert sich also nicht selbst, sondern bringt den Handybesitzer durch Irreführung dazu, die Aktivierung vorzunehmen. Zudem haben die Betriebssysteme von Mobiltelefonen, namentlich Windows CE und Symbian, bestimmte Sicherheitslücken, welche die Verbreitung und Installation von Schadprogrammen begünstigen.

**Formen von Handy-Dialern und Handy-Viren**
Zumindest bis jetzt (Stand: 2011) ist die Zahl von Programmen dieser Art überschaubar, ebenso die Zahl der konkreten Schadensfälle.
Als erster Handy-Virus ging **Cabir** in die Geschichte ein. Dieser Virus verbreitete sich über Bluetooth: Sobald das Handy angeschaltet wurde, verschickte sich Cabir selbstständig an Geräte mit offener Bluetooth-Anbindung in der Nähe.
Der erste Dialer-Trojaner für Handys verbreitete sich ebenfalls im August 2004, damals auf Mobiltelefonen mit dem Symbian-Betriebssystem Series 60. Der Trojaner verschickte ohne das Wissen des Handybesitzers SMS und steigert so die Telefonrechnung kräftig. Das Schadprogramm versteckte sich dabei in einer Raubkopie des Handy-Games Mosquitos, einer Moorhuhn-Variante des deutschen Entwicklers Ojom. Dabei handelte es sich freilich noch nicht um einen bewusst entwickelten Handy-Dialer: Der teure SMS-Versand war Medienberichten nach die Folge einer fehlgeleiteten Kopierschutzfunktion.
Konkreter wurde die Gefahr schon im Frühjahr 2005 mit dem Programm **ComWarrior**. Dieser Wurm tarnte sich hinter einer MMS-Nachricht. Öffnete man den Anhang, begann ComWarrior (ComWar) mit seiner Schadfunktion – der Weiterverbreitung per Versand an alle Adressbucheinträge des infizierten Handys. Dadurch konnten dem betroffenen Telefonbesitzer – je nach Umfang seines Handy-Adressbuchs – horrende Schäden entstehen. In einem im Januar 2006 bekannt gewordenen Fall beklagte ein Betroffener einen Schaden von 400 Euro. Auch er hatte ganz offensichtlich nicht bemerkt, dass sein Handy plötzlich und ungewollt etliche teure MMS verschickte.
Im Februar 2006 brachte dann ein Trojaner mit Namen **J2ME/RedBrowser.A** arglose Kunden der russischen Mobilfunkbetreiber MTS, Beeline und Megafon um ihr Geld. Wie der Antivirus-Hersteller Kaspersky berichtete, musste der 54482 Byte große Schädling als gewöhnliches Java-Archiv mit Namen "redbrowser.jar" auf Handys wie eine normale Applikation installiert und ausgeführt werden. Einmal gestartet gab der Handy-Dialer in einer auf Russisch verfassten Anleitung vor, WAP-Seiten per SMS ohne Datenverbindung abrufen zu können, wobei die ersten fünf Megabyte beziehungsweise 650 SMS kostenlos seien. Statt der WAP-Seiten bekam der Handybesitzer allerdings eine überhöhte Telefonrechnung präsentiert, da die gewählten netzinternen Premium-SMS-Nummern mit rund fünf US-Dollar pro Nachricht abgerechnet wurden. Deutsche Kunden waren von diesem Dialer nicht betroffen.
Im April 2006 tauchte **RommWar** erstmals auf. Der Trojaner überschrieb bei der – manuellen – Installation eine Systemdatei und sorgt dafür, dass diese beim nächsten Neustart des Handys ausgeführt wird. In der Folge sorgte RommWar dafür, dass bestimmte Gerätefunktionen ausfielen oder das Mobiltelefon überhaupt nicht mehr startete.
Ende 2009 tauchte der Trojaner **Java/Swapi.B** auf. Der Handydialer bestand Medienberichten zufolge aus einem Java-Programm, das auf den meisten Mobiltelefonen lauffähig war. In der Softeware waren teure Premium-SMS-Nummern hinterlegt. An diese sendete der Dialer dann heimlich und ohne Zutun des Handy-Besitzers SMS.

**Botnetze durch Handy-Trojaner**
Ab 2008 wurden auch Handy-Trojaner bekannt, die dazu geeignet waren, regelrechte Bot-Netze zu bilden. In diesem Fall könnten tausende und zehntausende Mobilfunkgeräte von einem Dritten, dem "Lenker" der infizierten Geräte, dazu missbraucht werden, einen Angriff auf ein Mobilfunknetz zu starten und dieses sogar lahm zu legen. Ziel der Aktion: Der Täter, der die Handys mit Trojanern infiziert hat, könnte die

Betreiber von Mobilfunknetzen erpressen nach dem Motto "Zahlt, sonst lasse ich einen Angriff auf euer Netz starten."

**Welche Handys sind betroffen?**

Handy-Dialer und ähnliche Schadprogramme benötigen ein leistungsfähiges Betriebssystem, um funktionieren zu können. Insofern sind alle moderneren Mobiltelefone (Smart-Phones) betroffen. Grundsätzlich gilt: Je mehr Möglichkeiten ein Handy hat, umso mehr Möglichkeiten haben auch Viren, Trojaner und Dialer, das Gerät zu infizieren und darauf aktiv zu werden.

**Woran erkenne ich, dass mein Handy oder mein Smartphone infiziert ist?**

Da die Zahl der Schadprogramme für Mobiltelefone bislang gering ist, lässt sich hier keine generelle Aussage treffen.

- Ein Alarmsignal ist mit Sicherheit, wenn Ihr Mobiltelefon ungewollt und ohne äußeren Einfluss plötzlich mit dem Versand von SMS, MMSoder Premium-SMS beginnt, bzw. Telefonverbindungen herstellt. Erkennbar ist dies entweder an den bekannten akkustischen Signalen (Pieps-Ton) oder am plötzlichen Aufleuchten des Displays.

- Ein ganz konkretes Anzeichen für einen Dialer- oder Trojaner-Befall sind natürlich unerwartete Posten auf der Mobilfunkrechnung. Tritt hier eine massive Häufung von Ihnen unbekannten Verbindungen oder Posten für den Kurznachrichten-Versand auf, sollten Sie misstrauisch werden. Das gilt vor allem dann, wenn Sie kurz zuvor neue Programme auf Ihrem Smart-Phone installiert haben oder Kurznachrichten (MMS) von Ihnen unbekannten Absender erhalten und geöffnet haben.

Schutz vor Handyviren und Handydialern

Aktuell sind keine Handyviren oder Handydialer bekannt, die sich selbst auf dem Mobilfunkgerät installieren und aktivieren. Insofern ist der beste Schutz gesundes Misstrauen und eine gewisse Vorsicht.

- Installieren Sie auf Ihrem Mobiltelefon niemals Programme, deren Herkunft und Funktionsweise Sie nicht kennen.

- Schalten Sie die Bluetooth-Verbindung an Ihrem Handy aus. Aktivieren Sie diese nur, wenn Sie sie wirklich benötigen und deaktivieren Sie sie anschließend wieder.

- Denkbar ist auch der Schutz durch spezielle Antiviren-Software für Handys. Eine Übersicht über die gängigen Programme finden Sie bei unseren Downloads. Dialer- oder Einwahlblocker für Mobiltelefone sind bislang nicht auf dem Markt.

**Ausblick und Entwicklung**

Die weiter zunehmende Verbreitung von mobilen Endgeräten wie Handys und die damit verbundenen neuen Möglichkeiten machen es sehr wahrscheinlich, dass auch die Zahl der auf Mobiltelefone spezialisierten Schadprogramme zunehmen wird. Damit verbunden werden sich dubiose Anbieter auch neue Formen der Abzocke überlegen. Voraussetzung für eine Verbreitung von kostspieligen Handy-Dialern wird allerdings sein, dass sich die Täter Möglichkeiten der Gewinnabschöpfung schaffen – dass sie also unmittelbar und finanziell von den Schadfunktionen profitieren können. Dies könnte sowohl bei Premium SMS, als auch bei der Telefonie über Premium-Nummern gelingen.

www.computerbetrug.de/telefonabzocke/handy-viren-und-handy-dialer

## Wozu dienen Bluetooth- und Infrarot-Anschlüsse?

Bluetooth ist eine Funktechnik zur drahtlosen Sprach- und Datenübertragung zwischen elektronischen Geräten im Nahbereich. Bluetooth wird zum Beispiel für kabellose Freisprecheinrichtungen genutzt oder um zwischen Handys Fotos und Videos zu tauschen.
Bluetooth soll die Infrarot-Schnittstelle ablösen. Bei einer Datenübertragung über Infrarot ist es notwendig, dass die Handys im richtigen Abstand unbewegt nebeneinander liegen und es kann auch nur eine bestimmte Datenmenge geschickt werden.
Der Bluetooth-Standard weist drei Klassen auf und kann etwa 10, 50 oder 100 Meter weit funken. Die meisten Handys haben eine Reichweite von etwa 10 Metern.
Verbindungsaufbau: Voraussetzung ist, dass Bluetooth eingeschalten und das Gerät für Bluetooth sichtbar ist. Sobald ein Bluetooth-Gerät aktiviert ist, beginnt es nach anderen zu suchen. Wenn sich zwei Bluetooth-Handys gefunden haben, können sie untereinander Daten austauschen. Dafür müssen jedoch beide Handy-BesitzerInnen das gleiche Passwort eingeben bzw. den Datentausch akzeptieren.
Damit dann eine Datenübertragung zwischen Bluetooth-Geräten wirklich funktioniert, ist es auch erforderlich, dass sie über die gleichen „Profile" verfügen. „Profile" legen fest wie genau Daten für einen bestimmten Zweck übertragen werden können, z.B. für Headsets oder Audio-Übertragungen.
Mit Bluetooth können Daten bis zu einer Übertragungsrate von 700 kBits/s im Frequenzbereich von 2,4 GHz übertragen werden. In Entwicklung ist ein Standard, der bis zu 100 MBits/s übertragen kann. Bluetooth wechselt bis zu 1.600-mal in der Sekunde die Frequenz innerhalb von 79 Frequenzstufen. Das verringert Funkstörungen und erhöht die Sicherheit.
Im Vergleich zur Infrarottechnik ist ein Sichtkontakt bei Bluetooth nicht unbedingt notwendig. Bluetooth-Geräte müssen während der Datenübertragung auch nicht stillgehalten werden.

http://handywissen.at/was-koennen-handys/#c302

## Bluetooth funkt auf kurzen Wegen

Bluetooth ist eigentlich dafür entwickelt worden, dass ein Handy ohne Kabel mit einem Zusatzgerät verbunden werden kann. So gibt es heute zum Beispiel Headsets und Freisprecheinrichtungen, die mit Bluetooth funktionieren. Bei Bluetooth werden Daten per Funk übertragen. Die meisten Handys haben auch eine Infrarot-Schnittstelle. Das funktioniert über Lichtsignale. Um Daten mit Infrarot zu tauschen, müssen sich die Handys also "sehen". Bluetooth funktioniert auch, wenn man das Handy in der Hosentasche hat. Allerdings funkt Bluetooth bei vielen Geräten nur auf eine Entfernung von etwa 10 Metern. Bluetooth gibt es nicht nur bei Handys. Auch Laptops, PCs und sogar manche Spielekonsole nutzen Bluetooth zum Austausch von Daten.

### Finde ein blaues Handy in deiner Nähe!

Jedes Handy mit Bluetooth-Funktion hat einen eigenen Namen. Das ist meist ein Produktname des Herstellers. Den Namen des Handys kann man allerdings auch selbst ändern. Mit einem Bluetooth-Handy kann man andere Geräte mit Bluetooth-Funktion in einem Umkreis von mindestens 10 Metern suchen, wenn keine Wände dazwischen liegen. Im Handy gibt es dafür eine Funktion zum Suchen von anderen Bluetooth-Geräten. Ein anderes Handy kann nur dann gefunden werden, wenn dort Bluetooth eingeschaltet ist. Außerdem kann der Bluetooth-Name auf unsichtbar geschaltet werden. Dann funkt das Handy seinen Namen nicht offen in die Welt hinein und kann nicht so leicht gefunden werden.

### Wenn die Handys sich paaren

Wenn sich zwei Bluetooth-Handys gefunden haben können Sie untereinander Daten austauschen. Dafür müssen jedoch beide Handy-Besitzer das gleiche Passwort eingeben. Die Verbindung zwischen den beiden Geräten ist dann verschlüsselt. Für die sichere Bluetooth-Paarung ist es wichtig, den Anweisungen der Geräte genau zu folgen. Wenn es möglich ist, sollten die sicheren Einstellungen aktiviert werden.
Achtung: Hintertüren bei Bluetooth
Bei Bluetooth werden Daten durch die Luft gesendet und empfangen. Leider kommt es immer häufiger vor, dass Hacker sich über diesen Funkweg Zugang zu fremden Handys verschaffen. Dann können die Daten (Adressbuch, SMS, Bilder) auf dem gehackten



Handy gelesen und verändert werden (BlueSnarfing). Außerdem kann über das fremde Handy telefoniert oder eine SMS verschickt werden (BlueBugging). Der Handy-Besitzer bekommt davon meist gar nichts mit. Ein anderer Angriff auf Bluetooth-Handys ist das sogenannte BlueSmack. Dabei werden alle anfälligen Geräte, die in Reichweite sind, gestört. Grundsätzlich kann jede Funkverbindung durch einen Störsender sabotiert werden (Jamming). Die Reichweite von Bluetooth-Handys beträgt normalerweise etwa 10 Meter. Andere Bluetooth-Geräte können über 100 Meter weit funken. Bei einer öffentlichen Vorführung wurde sogar schon ein Bluetooth-Angriff aus fast 2 Kilometer Entfernung durchgeführt. Für einen Hackerangriff werden meist Laptops mit entsprechender Software und spezielle Antennen genutzt. Allerdings gibt es auch Programme, um mit Handys einen Bluetooth-Angriff zu starten.

**Ich geh auf Nummer Sicher**

Um sich vor Hackerangriffen zu schützen sollte der Bluetooth-Name eines Handys auf unsichtbar gestellt werden. Dann ist es schwerer, das Handy zu orten. Allerdings gab es auch Angriffe auf Handys, deren Bluetooth-Name unsichtbar war. Denn die grundlegende Bluetooth-Funktion ist dann noch immer aktiv. Sicherer ist es, Bluetooth am Handy ganz auszuschalten, wenn es nicht benutzt wird. Besonders an öffentlichen Plätzen kann es gefährlich sein, wenn Bluetooth aktiviert ist. Außerdem sollte man sich gut überlegen, mit wem man eine Bluetooth-Paarung macht. Und wenn es keine dauerhafte Verbindung zwischen zwei Geräten sein soll, sollte die Verbindung nach dem Tausch von Daten wieder gelöscht werden. Sonst kann einem leicht etwas untergeschoben werden.

www.handysektor.de/index.php/aktuelles/netzwerk_more/immer_mehr_handys_machen_blau



# Mobile phone security: What are the risks?

June 17, 2011|By Amy Gahran, Special to CNN

The more people rely on cell phones and tablets, the more attractive these devices become as targets to thieves and other nefarious types.
Fortunately, protecting yourself against mobile security risks doesn't require getting paranoid about your phone. Rather, it's about maintaining good habits, watching for red flags and deciding whether you need mobile security tools or services.
At a recent mobile security conference in San Francisco, staffers from digital security provider Norton outlined some common current mobile threats:

Malware
This is an app contaminated with malicious code that makes your phone do things it shouldn't -- such as steal your personal data. While no smartphone platform is immune from malware, so far Android apps appear to present the greatest malware risk. This is because of the openness of this platform and Google's Android market.

This week, The Register reported on the latest rash of Android malware and noted that Google has admitted that „more than 90 percent of Android users are running older versions of the mobile operating system that contain serious kernel vulnerabilities. That gives attackers an easy way to bypass Android's security sandbox, which is supposed to limit the data and resources each app is allowed to access."
At the Norton conference, a presenter demonstrated how quick and easy it is to „trojanize" an Android app. He downloaded an existing legitimate app from the Android Market, viewed the source code, copied in some malicious code, renamed the app and uploaded the now-malware to the market -- all in about three minutes.

Mobile security tools such as Lookout or Norton Mobile Security (in beta) can help guard against Android malware by scanning apps and other programs and data on your phone.
However, the best way to protect yourself against malware is to read the list of permissions that an Android app requests before you install it. Does that list make sense? For instance, does a game really need to be able to send premium text messages or access your contact list?

It helps to understand what each of the available Android permissions mean and to check the apps already on your phone to spot excessive permission requests.
[....]

http://edition.cnn.com/2011/TECH/mobile/06/17/mobile.security.gahran/index.html





# 10 common mobile security problems to attack

By Michael Cooney, NetworkWorld

When it comes to security, most mobile devices are a target waiting to be attacked. That's pretty much the conclusion of a report to Congress on the status of the security of mobile devices this week by watchdogs at the Government Accountability Office. [...]

„Mobile devices face an array of threats that take advantage of numerous vulnerabilities commonly found in such devices. These vulnerabilities can be the result of inadequate technical controls, but they can also result from the poor security practices of consumers," the GAO stated. „Private [companies] and relevant federal agencies have taken steps to improve the security of mobile devices, including making certain controls available for consumers to use if they wish and promulgating information about recommended mobile security practices. However, security controls are not always consistently implemented on mobile devices, and it is unclear whether consumers are aware of the importance of enabling security controls on their devices and adopting recommended practices." [...]

The GAO report came up with a list of mobile vulnerabilities it says are common to all mobile platforms and it offered a number of possible fixes for the weaknesses. From the report:

Mobile devices often do not have passwords enabled. Mobile devices often lack passwords to authenticate users and control access to data stored on the devices. Many devices have the technical capability to support passwords, personal identification numbers (PIN), or pattern screen locks for authentication. Some mobile devices also include a biometric reader to scan a fingerprint for authentication. However, anecdotal information indicates that consumers seldom employ these mechanisms. Additionally, if users do use a password or PIN they often choose passwords or PINs that can be easily determined or bypassed, such as 1234 or 0000. Without passwords or PINs to lock the device, there is increased risk that stolen or lost phones' information could be accessed by unauthorized users who could view sensitive information and misuse mobile devices. [...]

Wireless transmissions are not always encrypted. Information such as e-mails sent by a mobile device is usually not encrypted while in transit. In addition, many applications do not encrypt the data they transmit and receive over the network, making it easy for the data to be intercepted. For example, if an application is transmitting data over an unencrypted WiFi network using http (rather than secure http), the data can be easily intercepted. When a wireless transmission is not encrypted, data can be easily intercepted.

Mobile devices may contain malware. Consumers may download applications that contain malware. Consumers download malware unknowingly because it can be disguised as a game, security patch, utility, or other useful application. It is difficult for users to tell the difference between a legitimate application and one containing malware. For example, an application could be repackaged with malware and a consumer could inadvertently download it onto a mobile device. The data can be easily intercepted. When a wireless transmission is not encrypted, data can be easily intercepted by eavesdroppers, who may gain unauthorized access to sensitive information.

Mobile devices often do not use security software. Many mobile devices do not come preinstalled with security software to protect against malicious applications, spyware, and malware-based attacks. Further, users do not always install security software, in part because mobile devices often do not come preloaded with such software. While such software may slow operations and affect battery life on some mobile devices, without it, the risk may be increased that an attacker could successfully distribute malware such as viruses, Trojans, spyware, and spam to lure users into revealing passwords or other confidential information.

Operating systems may be out-of-date. Security patches or fixes for mobile devices' operating systems are not always installed on mobile devices in a timely manner. It can take weeks to months before security updates are provided to consumers' devices. Depending on the nature of the vulnerability, the patching process may be complex and involve many parties. [...]

The GAO report went on to state that connecting to an unsecured WiFi network could let an attacker access personal information from a device, putting users at risk for data and identity theft. One type of attack that exploits the WiFi network is known as man-in-the-middle, where an attacker inserts himself in the middle of the communication stream and steals information. Communication channels may be poorly secured. Having communication channels, such as Bluetooth communications„open" or in„discovery" mode (which allows the device to be seen by other Bluetooth-enabled devices so that connections can be made) could allow an attacker to install malware through that connection, or surreptitiously activate a microphone or camera to eavesdrop on the user. In addition, using unsecured public wireless Internet networks or WiFi spots could allow an attacker to connect to the device and view sensitive information.

http://www.pcworld.com/article/2010278/10-common-mobile-security-problems-to-attack.html

# Wireless LAN Security Risks

By Alan Hughes, eHow Contributor

Wireless networks are relatively easy and inexpensive to set up today. In addition to many businesses that have installed wireless LANs, many people have installed wireless LANs in their homes and enjoy the benefits of connecting without cables. Unfortunately, the ease of wireless LAN and the nature of wireless technology may leave many users in homes and businesses with a network that is not secured, exposing their personal and business information to a drive-by cyber criminal.

**War Drivers**

"War driving" is a term that describes driving around looking for wireless networks. These cyber crooks drive through neighborhoods or business areas using their laptops to look for wireless network signals. When they find a network that is not secured, they attempt to hop on the connection. Once on the network, they target vulnerable computers and hack into them if at all possible or just passively "sniff" the network traffic looking for valuable information. One solution to this problem is to enable one of the wireless security methods on the wireless access point. WEP (wired equivalency protocol) is the easiest to enable and should be activated and configured to achieve at least minimal security.

**Rogue Access Points**

A particular problem in businesses is the deployment of rogue access points. Someone in a department may want to set up a wireless network in the office similar to what they have at home. If they are unwilling to wait for the information technology (IT) department to set one up, or worse, if they are unwilling to contact the IT department at all, such an installation may open the business up to network hacking. This is especially true if they do not activate any security protocols, such as WEP or WPA. Every business should have network monitoring tools in place to detect rogue access points

**Man-in-the-Middle Attacks**

Wireless hot spots are very popular and many restaurants offer free Internet access via their wireless network. Unfortunately cyber criminals also frequent these establishments. By setting up a wireless network ID that looks like what a customer might be expecting, they lure the unsuspecting victim into connecting to their "network." From that point the interceptor just forwards the network requests on to legitimate destinations while rummaging through the victim's laptop and stealing vital personal information. It is best to be alert when frequenting such a place, and be aware of any suspicious activity. Also be sure to connect to the business's valid network ID.

**Jamming**

Jamming occurs when a signal stronger than the signal produced by a wireless access point (WAP) is disrupted. This can be done deliberately by someone with bad intentions, or it can happen inadvertently if other wireless devices nearby interfere with the WAP's signal. Baby monitors, cordless phones and cell phones are all capable of "jamming" the signal of a wireless access point. Whether intentional or unintentional, jamming disrupts the wireless network and interferes with its proper operation.

www.ehow.com/list_6684310_wireless-lan-security-risks.html



# Mobile phone security

Attacks on Bluetooth-enabled devices can take place within a distance of 10 metres or more. [...]
As many as three-quarters of mobile phone users are not aware of the internet security risks linked to Bluetooth-equipped devices. These risks come in four main guises:

- Bluejacking is when anonymous text messages are sent to mobile phones
- Bluespamming is when a phone's contacts are secretly sent text messages
- Bluesnarfing is when hackers gain access to a mobile phone's contacts
- Bluebugging is when hackers have access to a handset's commands

While each of these risks is a nuisance, bluesnarfing and bluebugging are particularly serious. With bluesnarfing, hackers can gain access to stored data, such as a phonebook, calendar or to clone a phone.
Bluebugging, on the other hand allows hackers to make phone calls from the mobile phone they control. They can write messages and send them from the phone and they can even eavesdrop on private conversations. [...]

As with any mobile device, there are important precautions you can take to protect yourself against Bluetooth security breaches on a mobile phone:

- Always disable Bluetooth functionality on your phone when it's not in use
- Protect your phone with mobile antivirus software

By simply turning off Bluetooth, hackers are unable to mount your handset's commands or access the information on your Bluetooth-enabled mobile phone.

www.kaspersky.com/threats/bluetooth-risks