

Bedeutung Gaunerzinken:

Ihren Ursprung haben die Markierungen im „Rotwelschen“, einer Kriminellensprache, die im Mittelalter entstand. Im 16. Jahrhundert entwickelten sich daraus grafische Darstellungen, die an Häusern angebracht wurden, um Einbrechern oder Bettlern anzuzeigen, ob zum Beispiel die Eigentümer häufig zu Hause sind oder ob das Haus von einem Hund bewacht wird.



Bissiger Hund



Hier gibt es etwas



Hier gibt es Geld



Fromm stellen



Hier gibt es nichts



Betteln verboten



Alleinstehende Person



Alte Leute



Kein Mann im Hause



Übernachtung möglich

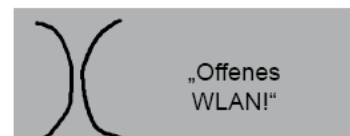
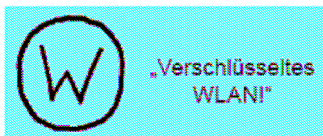


Frau liebt Männer



Vorsicht, nicht vorsprechen

Als „War-Chalking“ werden Markierungen bezeichnet, die auf ein an einem bestimmten Ort empfangbaren WLAN hinweisen. Sie geben teilweise sogar die SSID sowie das WEP-Kennwort an. Eingeweihte erkennen so schnell, wo man gratis Internet surfen kann. Diese sind angesichts der Hot Spots mittlerweile ebenso bedeutungslos wie die Gaunerzinken.



Sicherheitsregeln für Social-Network-Nutzer

Im Umgang mit den neuen Medien im Internet raten die Oberösterreichische Versicherung und die Sicherheitsdirektion Oberösterreich zu folgenden Sicherheitsmaßnahmen:

1. Niemals dasselbe Passwort für mehrere soziale Netzwerke verwenden, besonders nicht das für das primäre E-Mail-Konto und die Web-Konten.
2. Keinen Computer benutzen, bei dem nicht sicher ist, dass er frei von Viren oder Trojanern ist.
3. Immer die neuesten Updates und Patches für das verwendete Betriebssystem installieren, am besten automatisch.
4. Stets aktuelle Anti-Virus-, Anti-Malware- und Anti-Spam-Tools auf dem eigenem PC verwenden.
5. Vorsichtig sein bei Einladungen von »Freunden«, die man nicht kennt, und niemals Anfragen von völlig Fremden beantworten. Diese können von Spammern stammen oder Links auf Web-Seiten enthalten, die mit Viren oder Trojanern präpariert sind.
6. Keinesfalls persönliche Daten, wie etwa Handynummern oder den Wohnort, auf seiner öffentlichen Seite preisgeben. Solche Infos sind im Nachhinein schwieriger zu ändern als Instant-Messaging-Konten oder E-Mail-Adressen, falls einmal etwas schief geht.
7. Darauf achten, welche Infos man von sich preisgibt, wenn man seinem Profil Anwendungen hinzufügt und Funktionen für diese Anwendungen aktiviert. Wenn möglich nur Anwendungen von Unternehmen installieren, denen man vertraut und entsprechende Datenschutzeinstellungen verwenden.
8. Berufliches und Privates in Internet-Treffpunkten trennen! Keine Inhalte veröffentlichen, die einem später einmal peinlich sein könnten. (Unternehmen, bei denen man sich später bewirbt, können einem mit freizügigen Fotos aus der Jugendzeit oder Angaben über Hobbys und Vorlieben konfrontieren)
9. Vielfältige Möglichkeiten des Selbstschutzes im Internet beachten: gesetzliche Grundlagen, die den Datenschutz regeln, Einstellungsmöglichkeiten zum Schutz der Privatsphäre; Meldefunktionen in Sozialen Netzwerke in Anspruch nehmen