

## Vorsicht vor Phishing-Nachrichten nach Diebstahl von teuren Mobiltelefonen der Marke iPhone

### *Art der Bedrohung*

Diebstahl von teuren iPhones durch professionell agierende Taschendiebstahlsbanden – Zusendung einer Phishing-Nachricht für die „Lokalisierung“ des gestohlenen Gerätes.

### *Modus Operandi*

Wie intern vom LKA Steiermark berichtet, kommt es derzeit vermehrt zu Taschendiebstählen von teuren iPhones durch professionell agierende Diebstahlsbanden an stark frequentierten öffentlichen Plätzen, bei Großveranstaltungen, aber auch in Supermärkten und Gaststätten. Unmittelbar nach dem Taschendiebstahl erfolgt das Ausschalten des Gerätes durch die Täter, um eine Ortung via „find my iPhone“ unmöglich zu machen. Eine (Fern)Sperrung des Gerätes ist jedoch weiterhin möglich.

Da die Geräte in gesperrtem Zustand für die Täter nur einen Bruchteil des sonst zu erzielenden Wertes darstellen, werden die Geräte an IT-kundige Mittäter weitergegeben, welche versuchen das iPhone auf Werkseinstellungen zurück zu setzen. Dabei wird die für den Versand einer Phishing-Nachricht erforderliche Mail-Adresse und Telefonnummer dem Täter auf dem Display des Handy's angezeigt.

Im Falle einer aktiven Sperrung wird von den Tätern nach ca. 1-3 Wochen eine Phishing-Nachricht per Mail und SMS an den Bestohlenen versandt. In dieser Phishing-Nachricht wird behauptet, dass das Gerät von der Fa. Apple geortet wurde und man sich um auf den Standort zugreifen zu können, auf der („gefakten“) Homepage von Apple mit seinen Daten einloggen muss. Erliegt das Opfer dieser Täuschung und gibt seine Daten ein, stehen diese nun dem Täter zur Verfügung und können für die Rücksetzung und Entsperrung des Gerätes verwendet werden. Das Endgerät kann nunmehr ohne Einschränkung gewinnbringend veräußert werden.

Bleibt das Gerät weiterhin gesperrt, kann das Handy nur zerlegt und die Einzelteile als Ersatzteile verkauft werden, was bei Weitem nicht so lukrativ und viel aufwändiger ist. Das wird die Tätergruppierungen nicht unmittelbar von weiteren Straftaten abhalten, kann aber den auf die hochpreisigen iPhones abgezielten Diebstahl künftig unattraktiver machen.

### **Empfohlene Vorgangsweisen:**

- **Seien Sie vorsichtig** beim Erhalt von E-Mails, in welchen Sie aufgefordert werden „online“ die Standortdaten Ihres iPhone´s in Ihrer iCloud abzufragen, insbesondere wenn Ihnen ein solches vor kurzem gestohlen wurde.
- **Achten Sie darauf**, ob es sich um die tatsächliche Webseite von Apple handelt; kontrollieren Sie genau die Schreibweise der Domäne (<http://www.apple.xxx>).
- Haben Sie sich bereits „**irrtümlich**“ auf der „**gefakten**“ Seite eingeloggt, gehen Sie sofort auf die tatsächliche Seite von Apple und ändern Sie Ihr Zugangs-Passwort für die iCloud, bevor dies die Täter für Sie tun. Achten Sie dabei darauf, dass Sie eine gesicherte Verbindung zu Ihrem Account haben (<https://>).
- Kontaktieren Sie nach dem Erhalt einer solchen Phishing-Nachricht die Dienststelle, auf welcher Sie die Diebstahlsanzeige gemacht haben und geben Sie dort den Vorfall bekannt.
- Beachten Sie die Sicherheitshinweise und Tipps, für einen Sicherem Umgang mit dem Internet und Schutz vor IT-Kriminalität der Kriminalprävention: <http://www.bmi.gv.at>.
- Für weitere Informationen kontaktieren Sie die Cybercrime-Meldestelle im Bundeskriminalamt: [against-cybercrime@bmi.gv.at](mailto:against-cybercrime@bmi.gv.at).

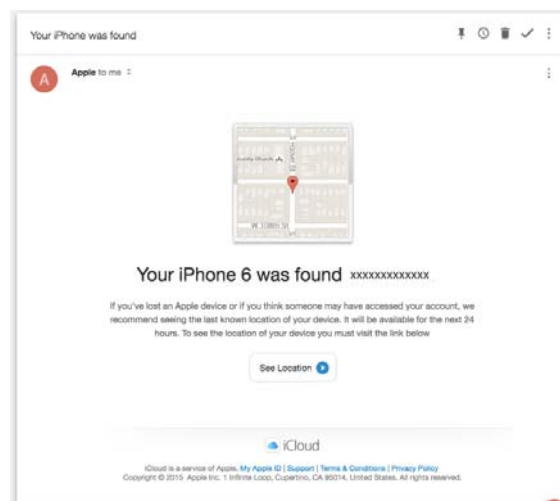
### Weiterführende und erklärende Links:

Watchlist Internet: Phishing mit gestohlenem iPhone (<https://www.watchlist-internet.at/phishing/phishing-mit-gestohlenem-iphone/>)

Hackernoon.com (englisch): This is what Apple should tell you when you lose your iPhone (<https://hackernoon.com/this-is-what-apple-should-tell-you-when-you-lose-your-iphone-8f07cf73cf82#.1ov2amwut>)

Dailymail.co.uk (englisch): Web Designer uncovers new scam thieves use to steal their victim´s identities (Story) (<http://www.dailymail.co.uk/news/article-3727379/Web-designer-uncovers-new-scam-thieves-use-steal-victim-s-identities.html>)

### Beispiele der Phishing-Nachrichten nach dem Diebstahl eines iPhone´s anhand einer E-Mail und SMS:



SMS with +1 (304)

Your iPhone was found. Click on the link below and login to view your iPhone's location: <http://show-iphone-location.com/>.

HERAUSGEBER: Bundesministerium für Inneres  
Bundeskriminalamt  
A-1090 Wien, Josef Halaubek Platz 1  
Tel.: +43 1 24836 986500

FEEDBACK

NEWSLETTER  
AN-/ABMELDUNG

Hinweis: Die vorliegende Information beruht auf einer Momentaufnahme aus dem Geschehen in der C4-Meldestelle ohne Berücksichtigung allen Falls vorhandener statistischer Daten aus dem Bundesgebiet und dient einem eingeschränkten Empfängerkreis zu Informations- und Präventionszwecken. Der beschriebene Tathergang sowie dazugehörige technische Details wurden im Rahmen der hier vorhandenen Möglichkeiten recherchiert und erheben keinen Anspruch auf Vollständigkeit. Angeführte Web-Links zu weiterführenden Artikeln und Informationen wurden zwar bei der Erstellung des Newsletters auf ihre sachliche und inhaltliche Richtigkeit überprüft, es besteht jedoch keine Haftung für das BK bei Änderung dieser Inhalte durch Dritte. Medienanfragen sind ausschließlich an die Pressestelle des Bundeskriminalamts zu stellen.