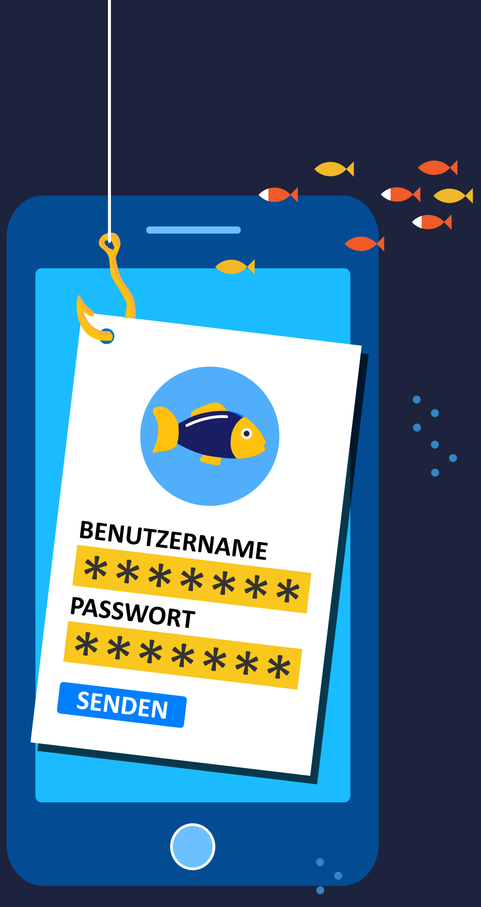
BEDROHUNGEN AUS DEM WEB

GENAU HINSCHAUEN, BEVOR SIE KLICKEN

Sie könnten Ihr Geld, Ihre persönlichen Informationen und sogar Ihre gespeicherten Daten verlieren, wenn Ihr Gerät nicht mehr funktioniert.



WIE KANN DAS PASSIEREN?

PHISHING ANGRIFFE: Verleiten Benutzer dazu, persönliche Informationen preiszugeben, indem sie sich als vertrauenswürdige Institution ausgeben. Sie verbreiten sich über E-Mail, Textnachrichten oder Social Media Plattformen.

WEBSITE BROWSING: Ihr mobiles Gerät kann bereits durch den Besuch einer unsicheren Website infiziert werden.

DATEIDOWNLOAD: Bösartige Links und Anhänge können direkt in eine E-Mail eingebettet sein.

WARUM IST DAS SO EFFEKTIV?

Mobile Geräte sind **STÄNDIG VERBUNDEN** mit dem Internet.

Die **REDUZIERTE GRÖSSE DES GERÄTBILDSCHIRMS** ist eine generelle Einschränkung. Mobile Browser zeigen URLs auf eingeschränktem Bildschirmplatz, wodurch schwer zu erkennen ist, ob es sich um eine legitime Domain handelt.

VORBEHALTLOSES VERTRAUEN DER NUTZER in den persönlichen Charakter eines mobilen Geräts.

WAS KÖNNEN SIE TUN?

Seien Sie misstrauisch, wenn Sie eine SMS oder einen Anruf erhalten, in dem nach persönlichen Informationen gefragt wird. Sie können feststellen, ob die Nachricht/der Anruf echt ist, indem Sie das Unternehmen direkt unter der offiziellen Nummer anrufen.

Wenn Sie mit Ihrem mobilen Gerät im Internet surfen, vergewissern Sie sich, dass die Verbindung über HTTPS gesichert ist. Das können Sie am Anfang der URL kontrollieren.

Klicken Sie nie auf einen Link/Anhang in einer unerwünschten E-Mail oder SMS. Löschen Sie diese sofort.

Seien Sie vorsichtig, wenn Sie auf einer Seite mit schlechter Grammatik, Rechtschreibfehlern oder geringer Auflösung landen.

Falls verfügbar, installieren sie eine Mobile-Security-App, die Sie bei verdächtigen Aktivitäten warnt.

EUROPOL EC3 European Cybercrime Centre

KASPERSKY

#MobileMalware