

Unbekannte verschenken „Filmgeld“

In Osterrode (Harz) tauchten 50 Euro Scheine auf, die allesamt gefälscht waren. Es handelte sich bei diesen um sogenanntes "Filmgeld". Also „Geld“ das in Spielfilmen verwendet wird und echt wirken soll, aber ansonsten absolut wertlos ist. Wer damit im Geschäft bezahlt oder es anderweitig in Verkehr bringt, muss demzufolge nach **StGB §146- 149** mit einer Strafanzeige rechnen

Die auf den ersten Blick "echt" aussehenden Scheine sind aber als „Filmgeld“ sofort daran zu erkennen, dass das bei echtem Geld vorhandene **Wasserzeichen**, das **Hologramm** und auch der **Sicherheitsstreifen** fehlen.

Schadsoftware im Umlauf

Kriminelle haben das Internet längst als Schauplatz für ihre Betrugs-maschen entdeckt.

Jetzt nutzen sie sogar die Tatsache, dass man sich auf vielen Webseiten **verifizieren** muss, um ihre Schadsoftware zu verbreiten. Eine ähnliche Masche gab es mit einem „**Sicher bezahlen**“-Button bei Kleinanzeigen.

Ein öffentliches Amt warnt mittlerweile vor der Gefahr durch die betrügerischen Captchas und gibt Hinweise, wie man sich schützt. Bei „**verifizieren**“ Vorsicht geboten

Die Masche läuft folgendermaßen ab:

Bereits mit dem Setzen des Häkchens beim „**Ich bin kein Roboter**“-Captcha wird ein schädlicher Befehl in die Zwischenablage kopiert.

Im zweiten Banner sollen Nutzer dann per Tastenkombination ein Windows-Eingabefeld öffnen.

Eine weitere Tastenkombination soll den schädlichen Befehl aus der Zwischenablage in das Eingabefeld einfügen und ausführen.

Der Server des Angreifers lädt dann eine Schadsoftware herunter und installiert sie, um den PC zu übernehmen und erheblichen Schaden anzurichten.

Europaweite Betrugsmasche "gestrandeter Touristen" mit „Bank-Apps“

Der oder die mutmaßlichen Täter sprechen Passanten an, sie brauchen z.B. dringend 1.000 Euro, haben aber kein Bargeld bei sich. Sie würden ihm in seinem Beisein zur Kontrolle stattdessen via Bank-App 1.000 Euro überweisen. Vor den Augen des Opfers täuschten sie durch Tippen am Handy in eine vermeintliche Bank-App eine Transaktion vor. Daraufhin hob das Opfer das Geld von seinem Konto ab und übergab es dem Unbekannten. Eine Gutschrift erfolgte nie.

Bevorzugte Betrugsörtlichkeiten:

Bahnhöfe oder Raststätten an Autobahnen.

Niemals dem Ersuchen nachkommen.

02.09.2025

Agressiv Vertreter schwätzen Ihnen neue Verträge auf

- Wenn Internet-Pishing nicht greift, versuchen es Betrüger neuerdings nach altem Rezept - direkt an der Haustür. Vertreter – **häufig angeblich von der „Telekom“** – behaupten, Sie hätten schlechten Empfang und man wolle Ihnen neue, verbesserte Verträge unterbreiten. Geben Sie keine Daten über sich wie Kontonr., Bankverbindung, Geburtsdatum u.ä. heraus.
- **Vorsicht bei Haustürverträgen:**
- **Widerrufsrecht:** 14 Tage nach § 312g, § 355 BGB (schriftlich per Brief, Fax oder E-Mail). **Rückabwicklung fordern!**
- **Form:** formlos, aber eindeutig; vermeiden Sie das Wort **„Kündigung“**, verwenden Sie vielmehr das Wort **Widerruf**
- **Kein Kündigungsrecht:** Der Vertrag wird **erst nach 14 Tagen** rechtskräftig, besteht also zum Zeitpunkt der „Kündigung“ nicht
- **Folge:** vollständige Rückabwicklung, als wäre der Vertrag nie geschlossen worden.