**Falsche Microsoft-Mitarbeiter**

„Wichtig: Microsoft tätigt nie unaufgeforderte oder nicht terminierte Anrufe,
auch nicht wegen angeblich auf dem PC befindlicher Schadsoftware und Viren!

Ziele der Täter:

1. Online Geldüberweisungen, beim Zahlungsvorgang wird der Betrag vom Täter erhöht
2. Gutscheincodes (Paysafeguthaben)
3. Geldtransfers per Western Union

Vorgehensweise:

1. Opfer soll Fernwartungssoftware installieren oder bereits installierte Software freischalten und dem Täter Zugriff auf den PC gewährleisten
2. Betrüger täuscht vor, Viren zu finden, auf dem Bildschirm werden Viren angezeigt
3. Wenn Opfer Verdacht schöpfen und keinen Wartungsvertrag abschließen, erpressen die Betrüger aus Frust mit der Löschung der Daten
4. Zur Wiederherstellung der Daten sollen die Opfer Geldleistungen erbringen
5. Bildschirme werden eingefroren oder bleiben schwarz
6. Über den Zugriff kann auch unbemerkt Schadsoftware installiert werden

Folgende Tipps sind zu beachten:

1. Sofort auflegen
2. Misstrauisch gegenüber Unbekannten sein, wenn kein Termin vereinbart wurde, im Zweifelsfall mit dem Unternehmen Kontakt aufnehmen
3. Zugriff auf PC verweigern
4. Keine Fremd-Software kaufen
5. Bei bereits gewährtem Zugriff auf Ihren PC:
   - Gerät sofort vom Netz trennen
   - Software deinstallieren
   - PC einem Sicherheitscheck unterziehen lassen

- ändern sie ihre Passwörter
- Polizei benachrichtigen
- Microsoft benachrichtigen