- Rufen Sie Verwandte unter der Ihnen bekannten Telefonnummer zurück.
- Geben Sie keine Details zu Ihren familiären oder finanziellen Verhältnissen preis.
- Wenden Sie sich sofort an die Polizei unter 110, wenn Ihnen die Situation verdächtig erscheint.

Mehr Tipps gegen den Enkeltrick (/themen-und-tipps/betrug/enkeltrick/)

Falsche Mitarbeitende des Gesundheitsamtes

Betrüger geben sich am Telefon als angebliche Mitarbeitende eines Gesundheitsamtes aus und fordern dazu auf, einen Corona-Test zum Preis von lediglich 5000-7000 € durchzuführen. Eine Abwandlung des Vorgehens ist, dass Täter unter dem gleichen Vorwand bei Betroffenen an der Haustür klingeln und so versuchen in die Wohnung zu kommen.

- Lassen Sie sich nicht darauf ein kostenpflichtige Tests auf Covid-19 an der Haustür und nach telefonischer Aufforderung durchzuführen.
- Fragen Sie Ihren Hausarzt oder das Gesundheitsamt, ob ein Test für Sie angeordnet wurde.
- Übergeben Sie kein Geld an vermeintliche Tester an Ihrer Haustür. Lassen Sie sich auch durch Drohungen nicht verunsichern.
- Lassen Sie keine Fremden in Ihre Wohnung. Bestellen Sie Unbekannte zu einem späteren Zeitpunkt wieder, wenn eine Vertrauensperson anwesend ist.
- Wehren Sie sich energisch gegen zudringliche Besucher: Sprechen Sie sie laut an oder rufen Sie um Hilfe.
- Bei akuter Bedrohung rufen Sie die Polizei unter 110.

Wenn Sie Opfer von Betrug geworden sind (/opferinformationen/opferrechte/)

Falsche Microsoft-Mitarbeiter haben es auf Personen im Homeoffice abgesehen

Betrug durch falsche Mitarbeitende von Microsoft gibt es bereits seit einigen Jahren. Nun haben sich die Täter auf die aktuelle Situation während der Corona-Pandemie und den vielen Personen im Home-Office eingestellt. Sie geben vor, Mitarbeitenden bei "My IT Department" oder "from my Company" zu sein. Die Täter und Täterinnen sprechen oft englisch mit indischem Akzent. Sie versuchen die Angerufenen dazu zu bewegen, u.a. eine Fernwartung zu installieren.

So schützen Sie sich vor dieser Masche:

- Gewähren Sie Fremden keinen Fernzugriff auf Ihren Computer.
- Seriöse Unternehmen wie Microsoft nehmen unaufgefordert keinen Kontakt zu Kunden auf. Sollte sich ein Servicemitarbeiter ungebeten bei Ihnen melden, legen Sie auf.
- Sollten Sie Opfer geworden sein: Schalten Sie den Computer aus und trennen Sie den Rechner vom Internet.
- Ändern Sie über einen nicht-infizierten Rechner unverzüglich alle Passwörter.
- Erstatten Sie Anzeige bei der Polizei und Meldung bei Microsoft unter www.microsoft.com/de-DE/concern/scam (https://www.microsoft.com/de-DE/concern/scam).

Tipps für Unternehmen:

- Sensibilisieren Sie Ihre Mitarbeitenden im Homeoffice für die aktuelle Gefahr.
- Sorgen Sie dafür, dass Ihre Mitarbeitenden die eigenen IT-Hotline-Mitarbeiter kennen. Richten Sie auch für solche Fälle eine Hotline ein, die Ihre Mitarbeitenden anrufen können.
- Wer Opfer geworden ist, sollte den Rechner von der eigenen IT-Sicherheit überprüfen lassen.