- **Phishing-Attacken**

Wer von Euch kennt sie nicht? Die guten alten Phishing-Mails. Betrüger:innen ahmen beispielsweise ein Zahlungserinnerungsmail nach oder ein Mail eines Versandanbieters wie zB Amazon und geben an, es gebe ein Problem, um dieses zu beheben sollen persönliche Informationen wie etwa Kreditkartennummern oder die Adresse angegeben werden. Am besten: Nicht reagieren! Seid Ihr unsicher, dann fragt bei den offiziellen Kontaktmöglichkeiten des jeweiligen Unternehmens nach. Das Gleiche gilt für Werbemails, die nach persönlichen Informationen verlangen, um beispielsweise einen „Gewinn" ausbezahlen zu können.

- **Betrügerische Werbeanzeigen**

Diese werden meist über gehackte Accounts auf Social Media geschaltet. Klickt Ihr auf die gefälschte Werbeanzeige werdet Ihr auf eine Betrugsseite weitergeleitet. Im schlimmsten Fall kann sich sogar ein Malware-Download aktivieren. Daher: lieber Vorsicht als Nachsicht und nichts anklicken, was auch nur im Entferntesten unseriös wirkt.

- **Gefälschte Webseiten**

Gerade um diese Zeit im Jahr nutzen Hochstapler die Shoppinglaune aus. Darum informiert Euch am besten vor einem Kauf über Erfahrungen anderer Kund:innen mit der Website/Verkäufer bzw. überprüft das Impressum, denn im deutschsprachigem Raum müssen Onlineshops ein Impressum mit Name, Adresse etc. vorweisen. Ist dieses nicht vorhanden, dann lieber Finger weg. Wenn es vorhanden ist, aber die Website an sich unseriös wirkt, dann die Impressumsangaben und Seitennamen nutzen, um mittels Suchmaschine zu überprüfen, ob bereits Beschwerden zu dieser Website vorliegen.

- **Erfundene Gutscheincodes und Wertgutscheine**

Wenn Ihr auf einen falschen Rabatt klickt, kann ein Installer auf Euer Gerät heruntergeladen werden, was wiederum einen Banking-Trojaner herunterlädt und installiert. Seriöse Gutscheincodes und Wertgutscheine werden üblicherweise über die offiziellen Kanäle des Anbieters, zB über eine App veröffentlicht.

- **SMS-Packet-Betrug**

Gerade die Vorweihnachtszeit ist oft auch eine Paketzeit. Darum wird man hier leider schnell zum Betrugsopfer. Man erhält SMS mit durchaus seriös wirkenden Absendern wie zB DHL oder auch UPS, meist mit einem Link und einem Text aller „letzte Chance zum Abholen". Zumeist wird über diese Masche versucht, an Bankdaten zu kommen. Klickt man auf den Link, gelangt man meist auf eine Website, die einen auffordert, eine bestimmte App zu installieren. Ziel ist aber nicht aufzuzeigen, wo sich besagtes Paket befindet, sondern Bankdaten zu stehlen. Daher: App auf keinen Fall installieren. Denn durch die Installation hat man meist nicht nur selbst die gefährliche Schadsoftware am Gerät, sondern es wird den Betrüger:innen auch ermöglicht, diese Schadsoftware weiterzuverbreiten. Die genützte Telefonnummer für den Versand solcher SMS gehört meist Personen, deren Gerät bereits infiziert wurde.

Solltet Ihr den Link geklickt haben, ist das bei den momentan bestehenden Varianten dieser SMS noch keine große Gefahr. Am besten SMS mit der Nachricht löschen.

Habt Ihr die App runtergeladen und installiert und eventuell diverse Zugriffsberechtigungen erteilt, gilt es spezielle Vorkehrungen zu treffen: Telefon in den Flugmodus versetzten, damit die Schadsoftware keine SMS von Eurem Gerät verschicken kann. Danach die Schadsoftware von Eurem Gerät restlos entfernen. Dies verlangt zumeist das Gerät auf die Werkseinstellungen zurückzusetzen. Prinzipiell gilt aber immer, wenn Ihr Euch unsicher seid, fragt in einem Shop Eures Mobilfunkbetreibers nach.

Wartet Ihr auf ein echtes Paket von DHL oder einem anderen Versandanbieter, dann könnt Ihr mit der Paketnummer den Aufenthaltsort auf der echten Website des Paketservices lokalisieren.