# Sicherheit für Privatpersonen

w1ntermute

October 26, 2022

## 1 Wer wir sind?

- Ehrenamtlich tätig
- Eine bunte Gruppe von Aktivistinnen
- Frei und unabhängig. Eine Cryptoparty ist ein Zusammentreffen in netter Atmosphäre, bei dem Menschen mit Erfahrung anderen beibringen sicher mit E-Mail und Chat zu kommunizieren und ihre Festplatten zu verschlüsseln.

## 2 Begiffe

- Phishing, nachrichten um Daten zu erhalten oder schadcode auf dem betroffenen aus zu führen
- Spam, Nachrichten die in unnötigen Mengen verschickt werden. Keine harte abgrenzugn zu Werbung
- Spearphishing ist eine Attacke die gezielt auf einen kleinen Personenkreis zielt

# 3 Warnung

Ihr seht gleich reale Beispiele. Keine der gezeigten Links, sollten im Browser geöffnet werden.

# 4 Pishing

- Viele kennen es mittlerweile.

## 4.1 Phishing Passwort vergessen

## 4.2 Was sollten wir tun?

- Ruhe bewahren
- Die E-Mail in ruhe durchlesen
- Hab ich selber diese E-Mail veranlasst?
- Wann wurde diese E-Mail verschickt?

## 4.3 Die zeichen

## 4.4 Die Zeichen

- Nicht normale zwichen verwenden (nicht ASCII)
- Link führt zu einer Website
- Bilder können nicht geladen werden. (Kann aber auch vom Mailprogramm unterbunden werden)
- Kann auch von einer nicht bösen domain stammen. Passiert bei schlecht abgesicherten Websites.

## 4.5 Anderes Beispiel

`./images/Phishing_beispiel_gezielt.webp`

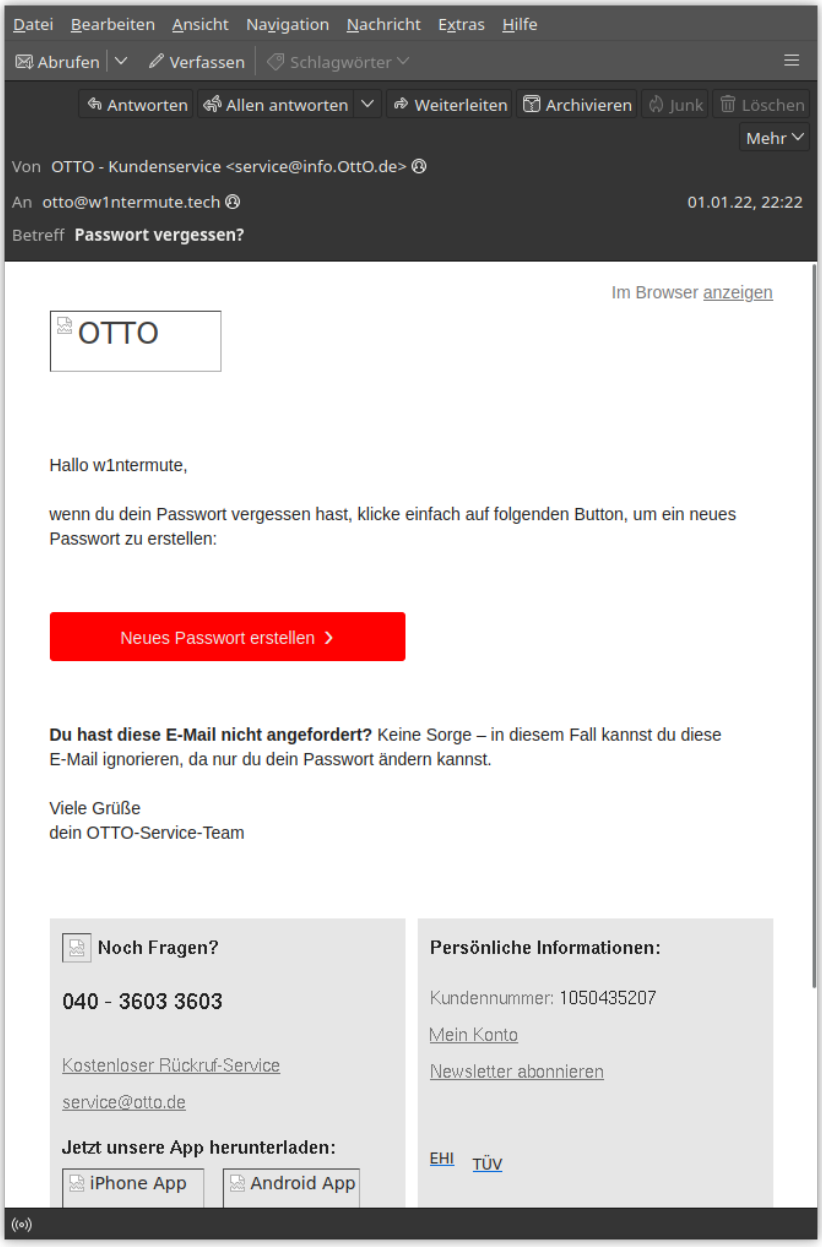


Figure 1: Passwort vergessen email

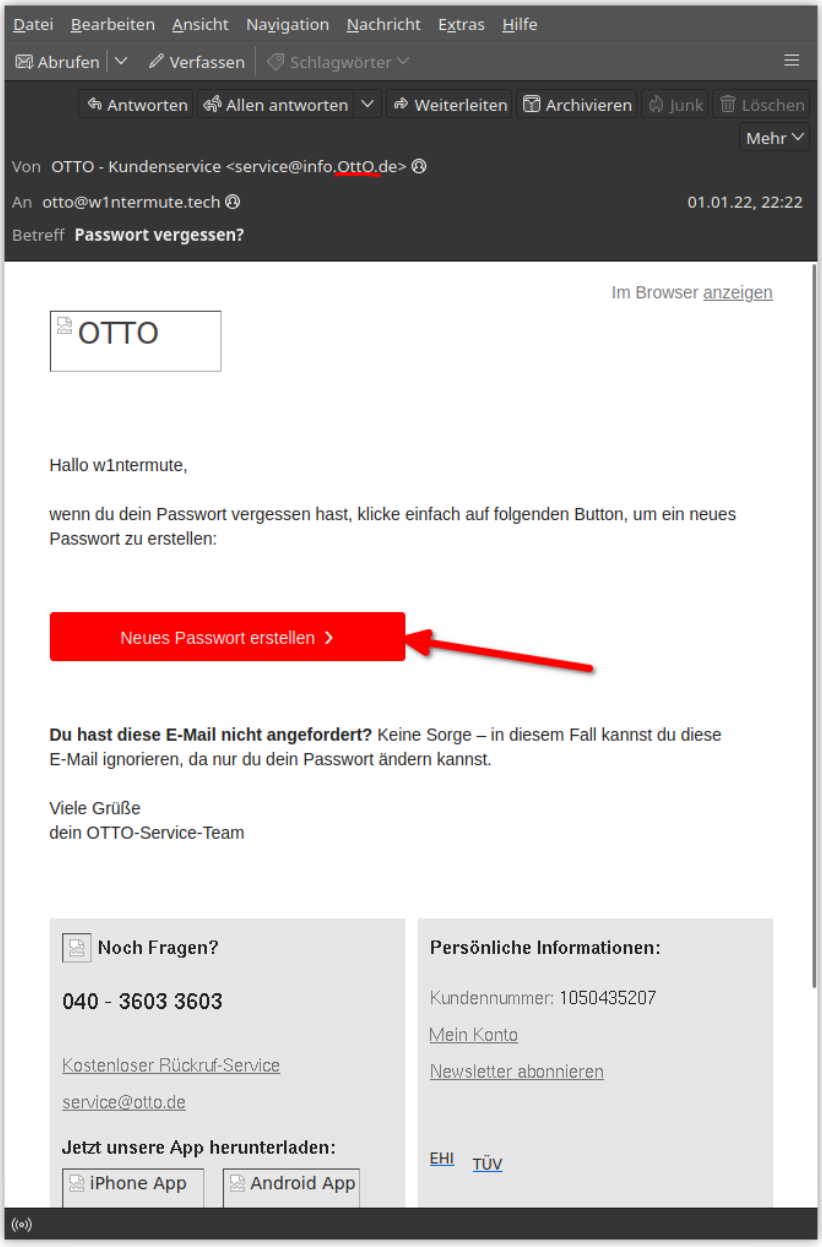


Figure 2: Passwort vergessen mit anmerkungen

### 4.6 Zeichen

- Text versucht Interesse zu wecken
- Anhang enthält dabei oft Mailware
- Betreff oft sehr generisch
- Zeitpunkt zu Uhrzeiten an denen wir schlecht Situtationen einschätzen können
- Versucht uns unter druck zu setzen oder kurzschlussreaktionen auszulösen.

### 4.7 Was kann ich dagegen tun?

- Erstmal überlegen. Habe ich diese E-Mail erwartet?
- Versuche über einen anderen kommunikationskanal den Absender zu verifzieren (Anruf,Chat)
- Öffne E-Mails im text format um Links besser zu sehen
- Versuche selber E-Mail in text statt HTML zu schreiben
- Sei bei E-Mails außerhalb deines Bekannten- oder Organisationskreises vorsichtig

### 4.8 Weite Informationen

- Verbraucherzentrale Phishing kampagnen und Phishing melden
- BSI

### 4.9 Umfrage

Welcher Firmenname wird momentan am häufigsten für Phishing genutzt?

- A: Microsoft
- B: DHL
- C: Google

### 4.10 Antwort

- DHL mit 23%
- Microsoft 20%
- Google 10%

## 5 Smishing

- Ist nichts anderes als Phishing für SMS
- Wird momentan mehr und mehr
- Wird auch genutzt um 2FA zu umgehen
- Ansonsten gelten hier diesselben regeln wie bei Phishing

### 5.1 Beispiel Pishing

> Hallo Christian, zeitlich begrenztes Angebot – 400 % Bonus + 100 Wolf Gold Freispiele! » `http://biy.io/d3ef32dd` Antworten Sie mit „STOP“, um sich abzumelden.

Hinweis: Gesendet um 02:00

### 5.2 Was sollten wir beachten?

- Auch hier wieder Kopfeinschalten. Es gibt nichts umsonst.
- Gesendet um 02:00 Nachts. Nachricht hofft das wir müde sind und einfach klicken.
- Information versucht wieder emotionale Reaktion hervor zu rufen.

### 5.3 Ziel

- Hinter dem Link steckt eine Website.
- Diese versucht uns eine App anzudrehen.
- App verteilt Malware

### 5.4 Nächstes Beispiel

Bitte bestätige deinen Login.

O Bestätige X Abweisen

Gesendet um 00:30

### 5.5 Was sollten wir beachten?

- Hab ich mich gerade irgendwo eingeloggt?
- Hab ich überhaupt einen Account bei diesem Service?
- Wenn ja, warum versucht sich jemand dort gerade anzumelden

### 5.6 Was ist zu tun?

- Jemand versucht gerade uns dazu zu bringen 2FA zu bestätigen
- Nachricht nicht bestätigen
- Passwörter wechseln

### 5.7 Was wird die Zukunft bringen?

- Voraufgenommene Videos von bekannten in einem chat.
- Deepfake phishing
- Angriffe werden immer besser. Kaum noch Rechtschreibfehler.
- Spear Phishing wird einfacher

## 6 Scam calls

### 6.1 Die momentan häufigste Fall

- Anrufer behauptet, eine gute Investitionsmöglichkeit zu bieten
- Anrufer behauptet von Europol zu sein. Eurpol ruft niemals euch direkt an.

### 6.2 Methodik

- Meist geht es dabei darum, Geld oder Informationen zu erlangen
- Niemals unter druck Informationen preis geben.
- Niemals Bankdaten über das Telefon preis geben.
- Wie schon bei den anderen Methoden. Vergewissert euch wer an der Leitung ist.

### 6.3 Was tun wenn man angerufen wurde?

- Bei der Polizei melden. Auch wenn Angriff nicht erfolgreich war.
- Es gibt mittlerweile Onlineportale bei der Polizei für diesen zweck. Beispiel Hamburg.
- Europol warnt und sammelt bekannte muster

### 6.4 Wie kann man sich schützen?

- Pflegt eure kontakte. E-Mail Adresse. Telefonnummer etc. Programme zeigen oft an ob etwas aus dem eigenen Kontaktbuch stammt.
- Ihr könnt immer auf einen anderen Weg die andere Person verifzieren.
- In Firmen, schafft abgetrennte Dienste. Die keine kommunikation von außen zu lassen.

### 6.5 Und immer an die Basics denken

- Regelmäßig eure Software updaten
- Schützt eure Information. (E-Mail,Telefonnummer). Nicht jeder braucht diese Informationen
- Für E-Mails gibt es dienste um alternative Adressen nutzen zu können.
- Für Telefon gibt es bestimmte Nummern die ihr angeben könnt Frankgehtran.