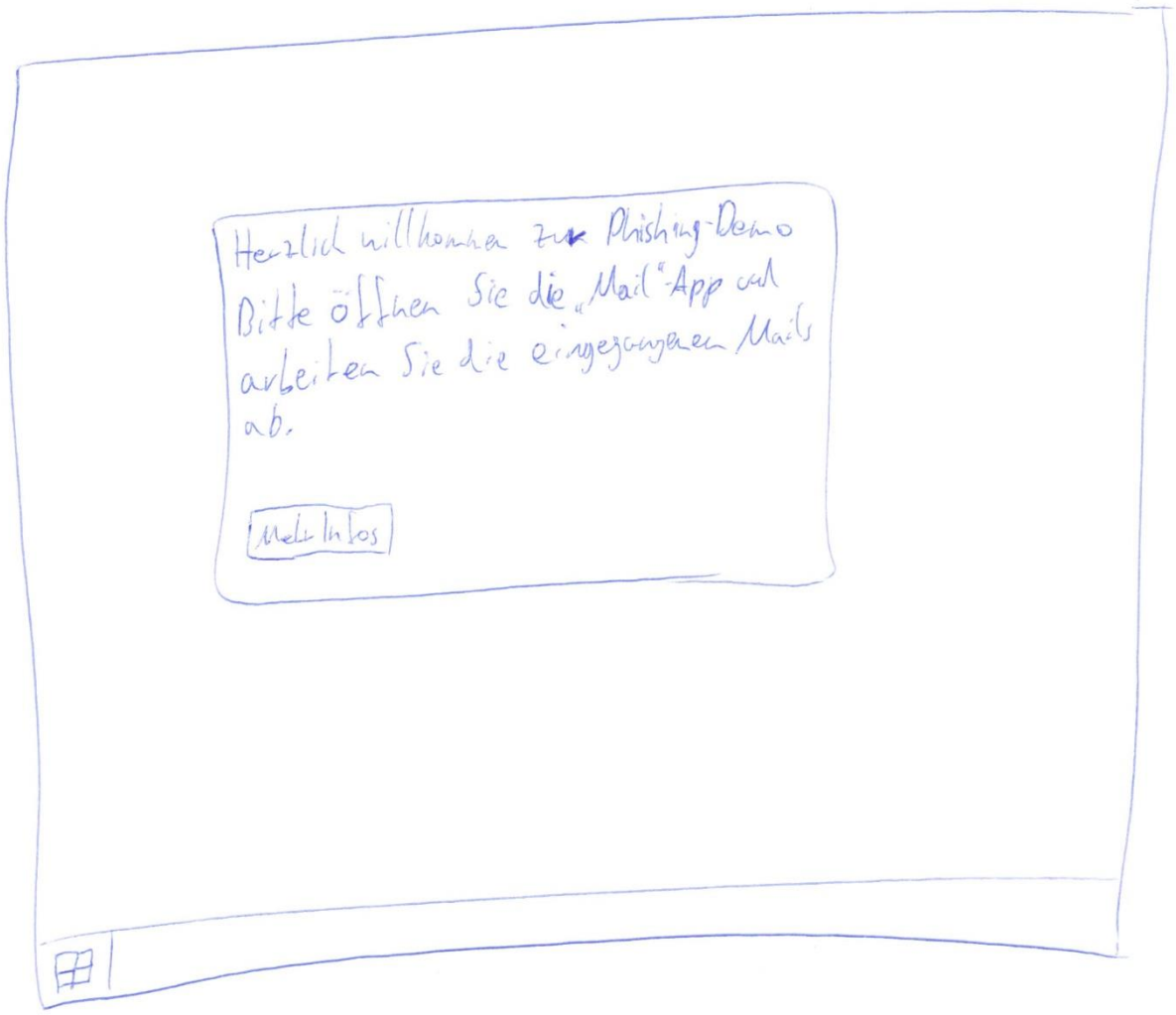
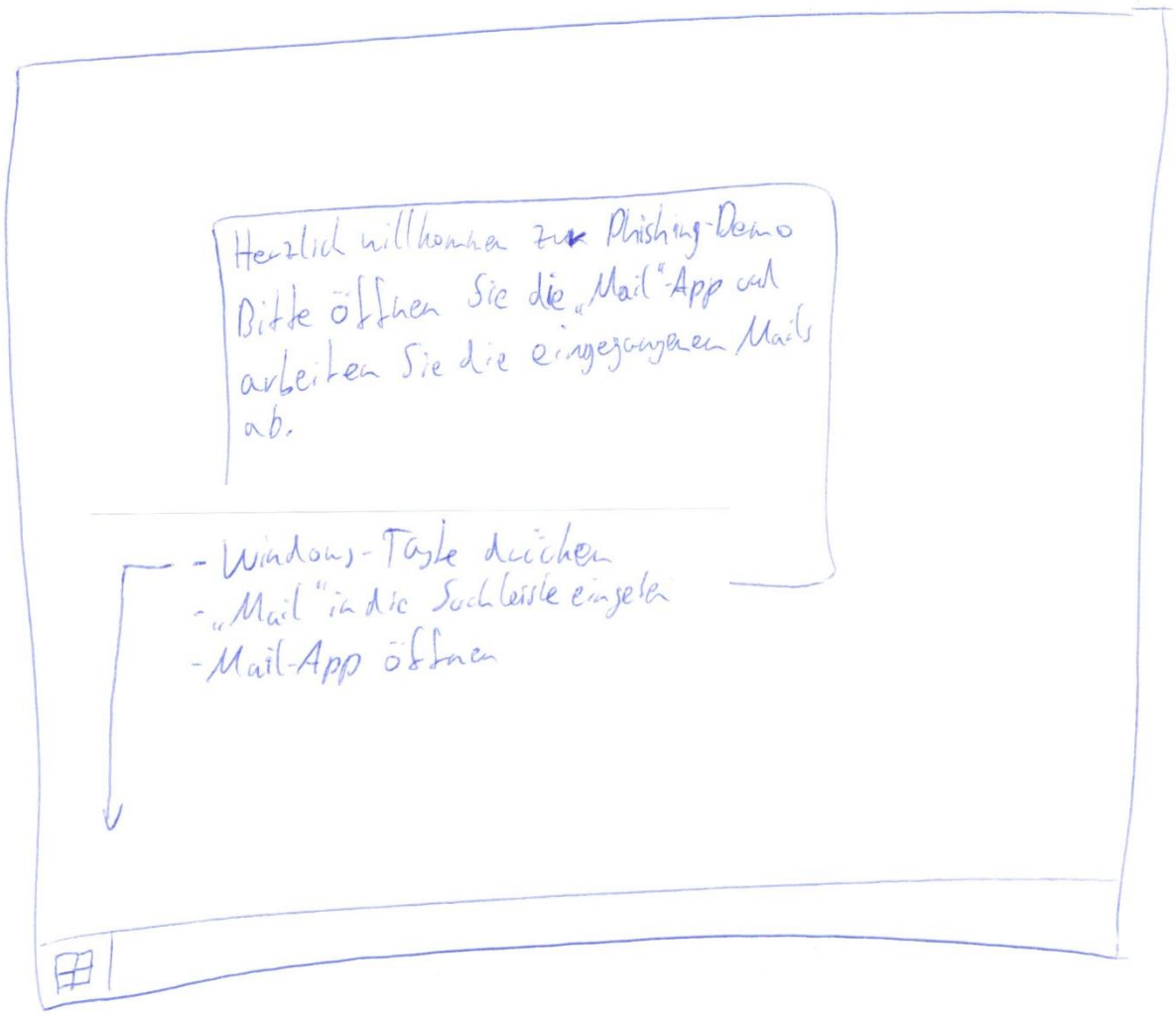
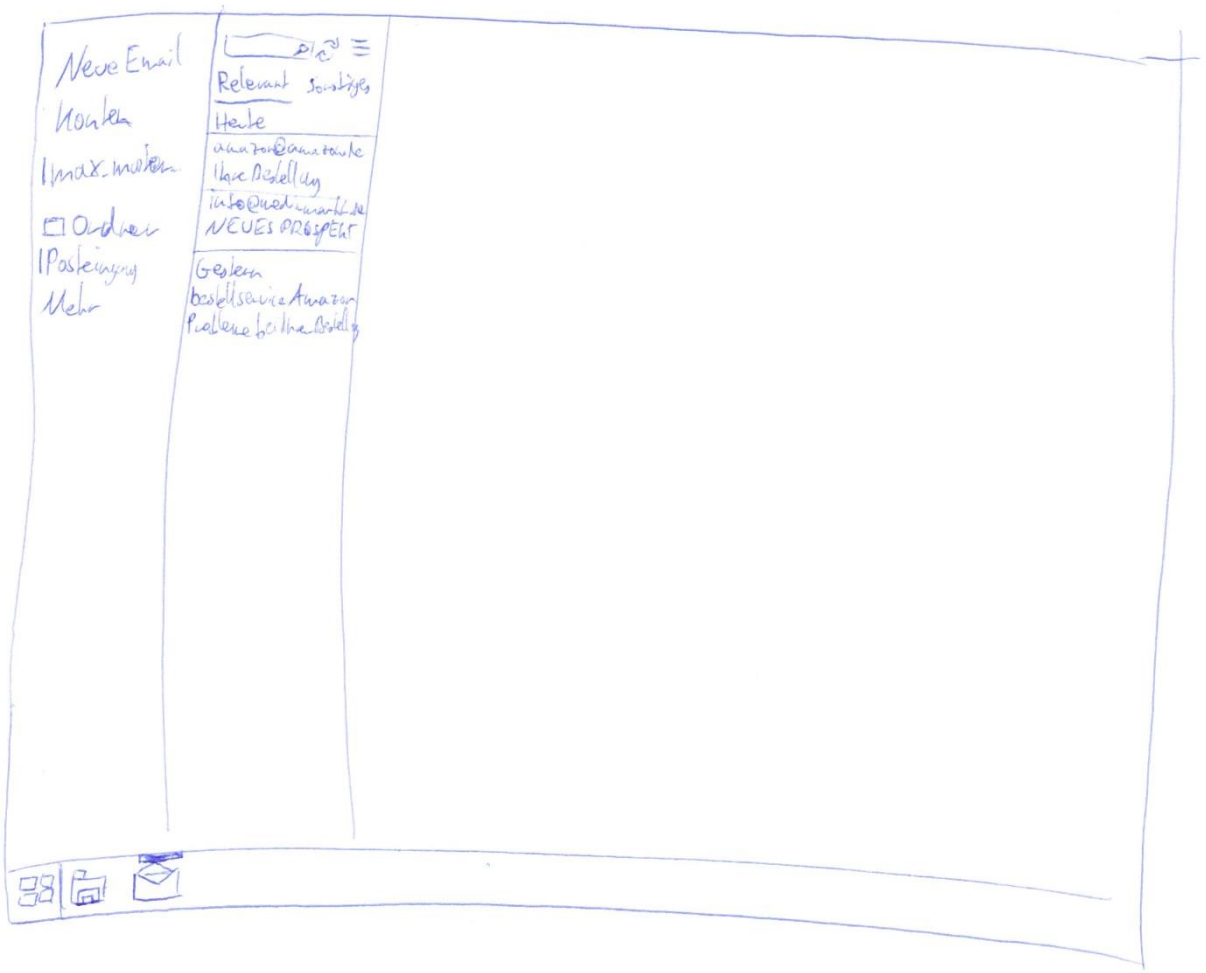
Demonstration Phishing



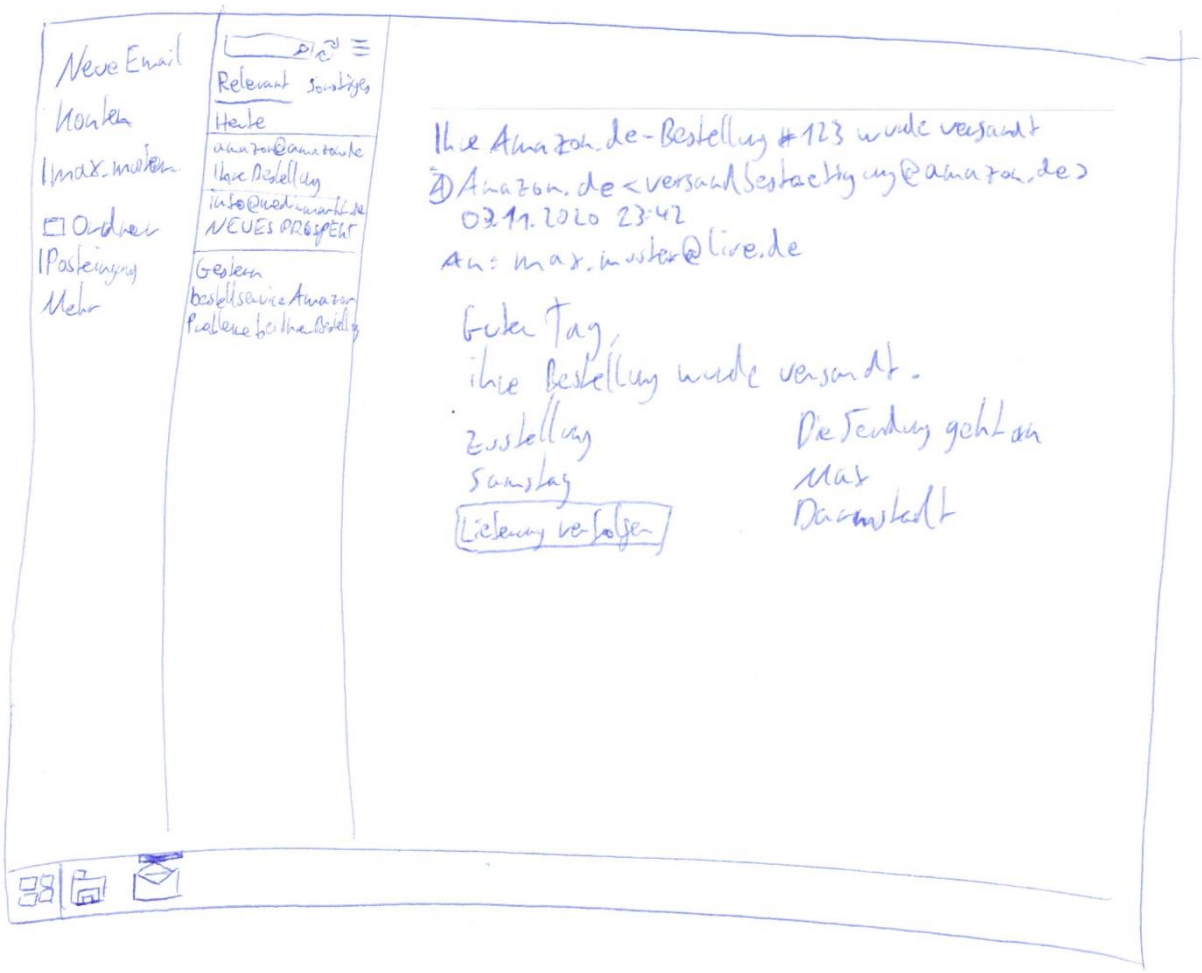
Nutzer wird kurz begrüßt und erhält die Aufgabe, das E-Mailprogramm zu öffnen und vorhandene E-Mails abzuarbeiten.



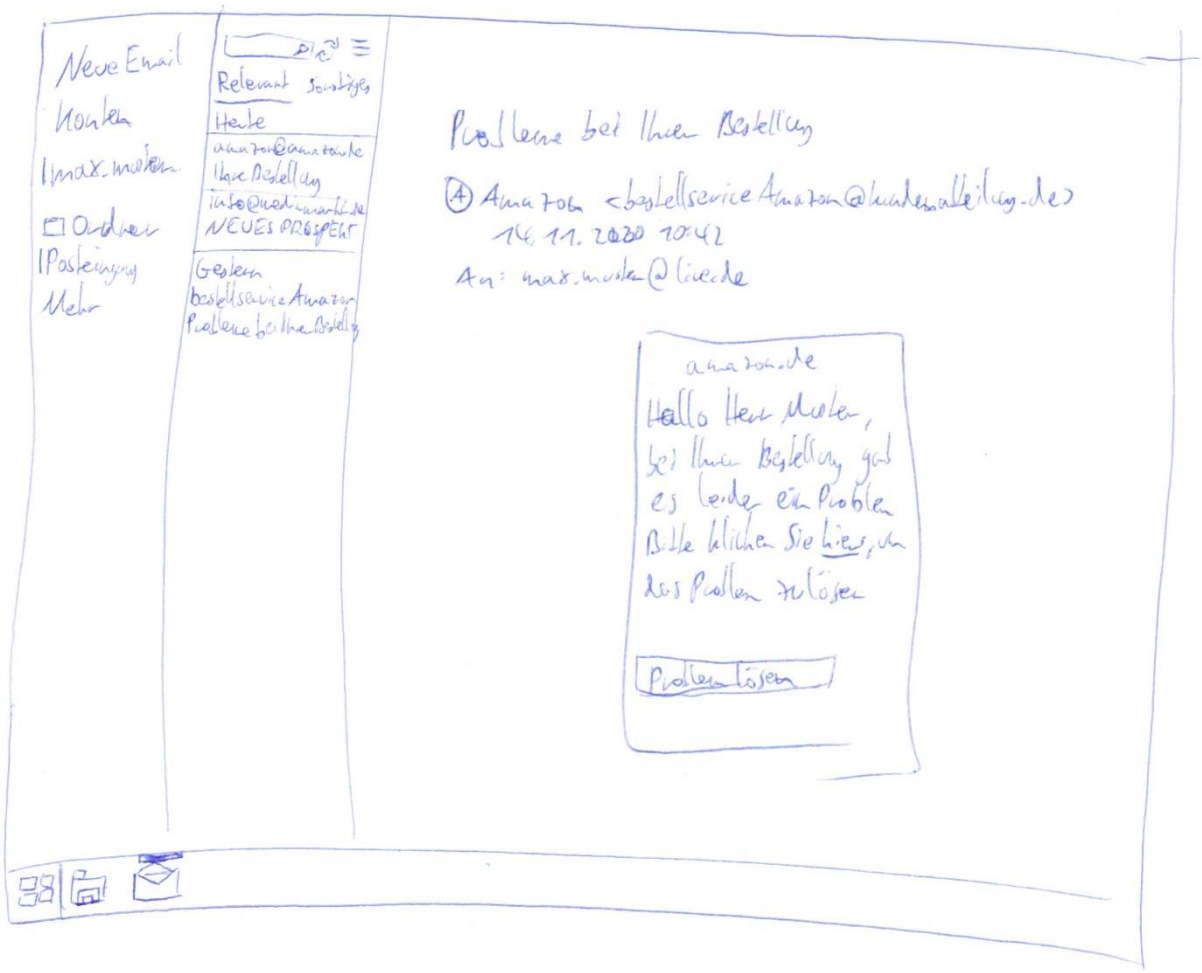
Mit „Mehr Infos“ kann sich der Nutzer noch Hinweise zum Ausführen der Aufgaben anzeigen lassen.



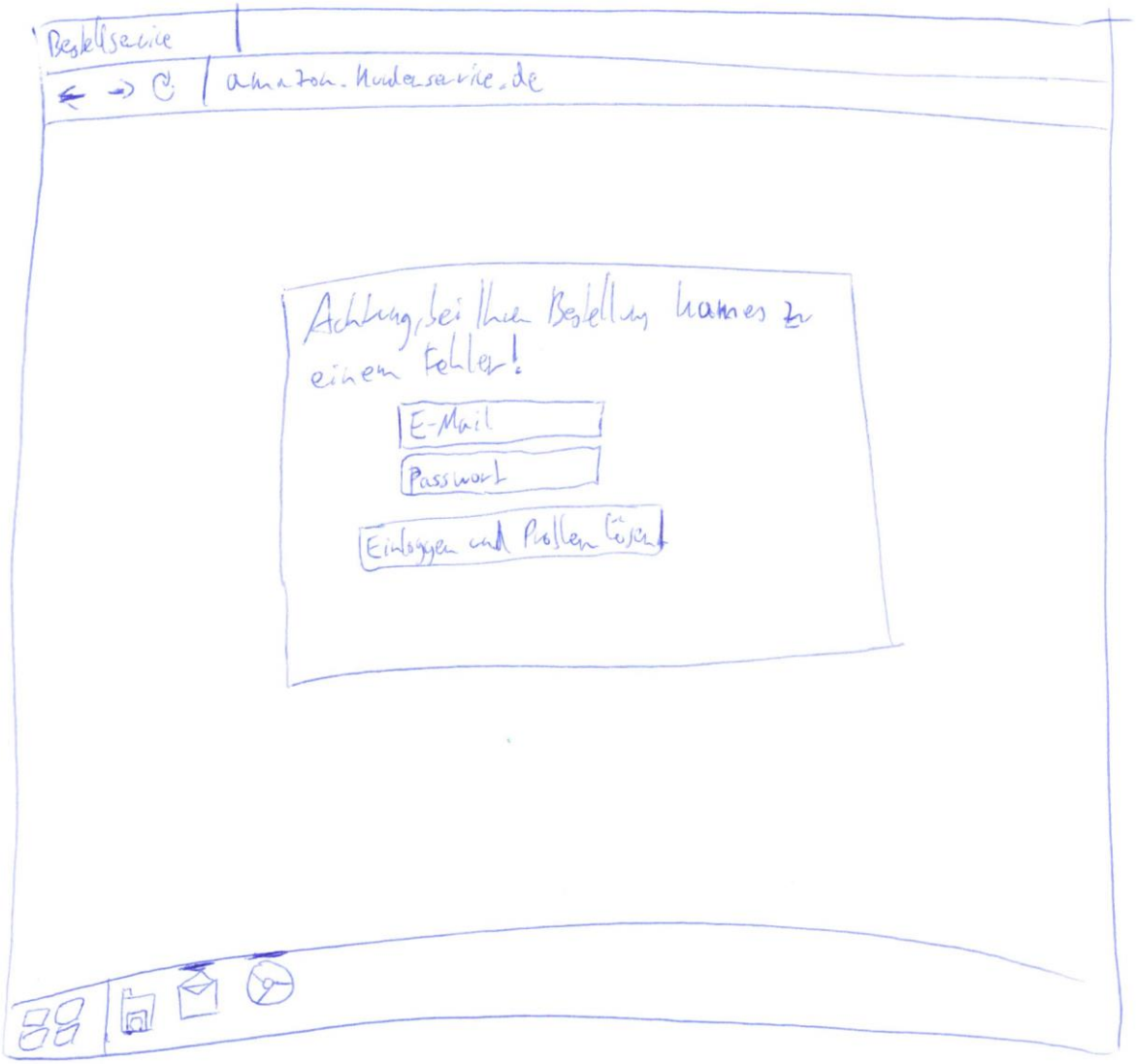
Der E-Mail-Client hat einen vorinstallierten Nutzer und mehrere eingegangene E-Mails.



Einige der E-Mails sind legitim.



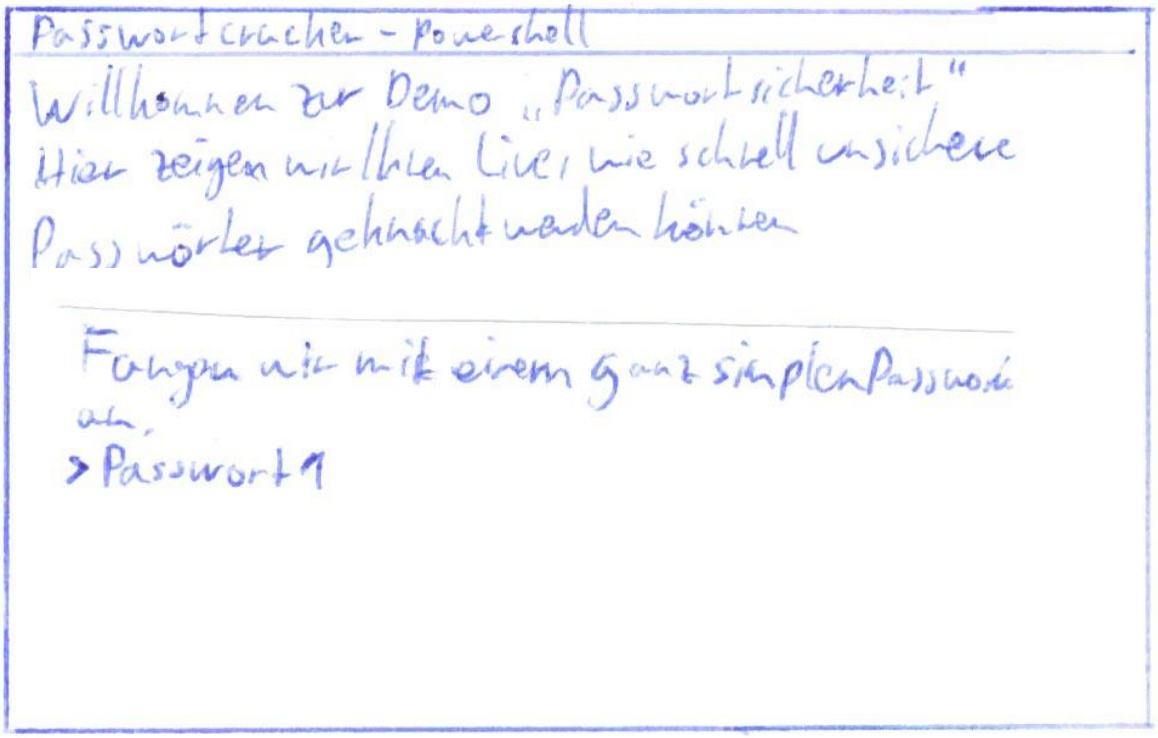
Andere E-Mails sind mehr oder weniger offensichtliche Phishing-Mails und enthalten Links auf potentielle Phishing-Seiten.



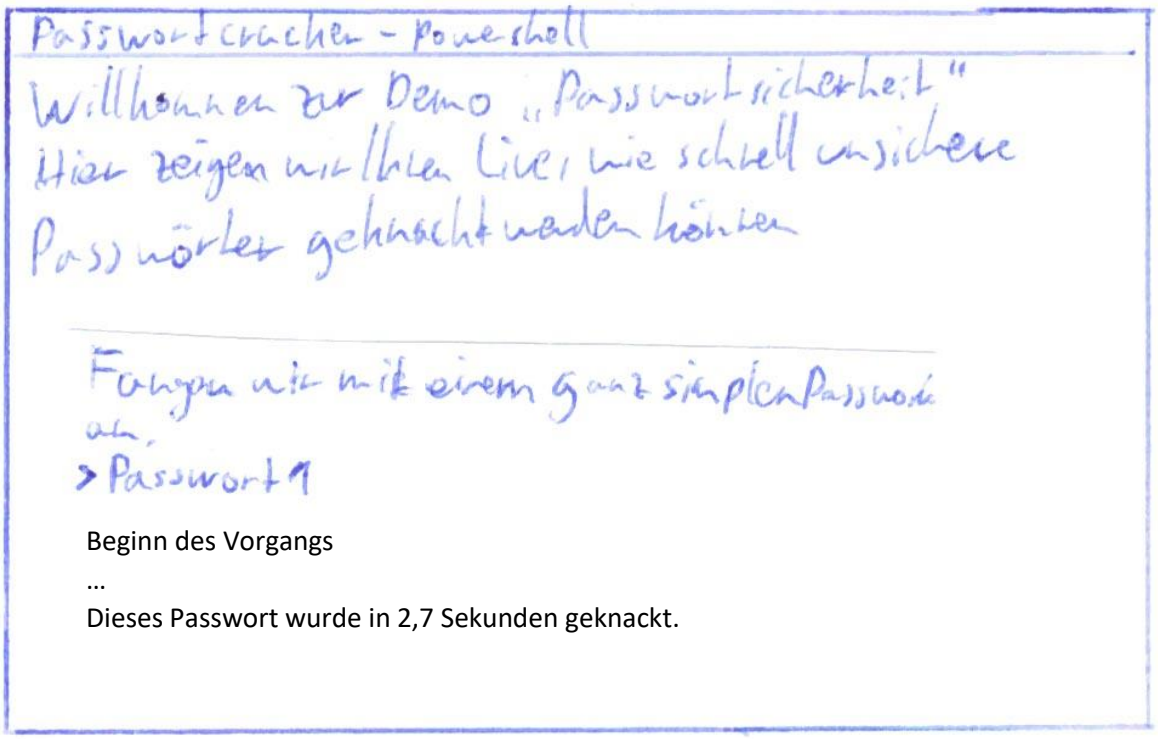
Die Phishing-Seite ist geöffnet und drängt den Nutzer sich vermeintlich mit seinen Kundendaten anzumelden, damit diese abgegriffen werden können.

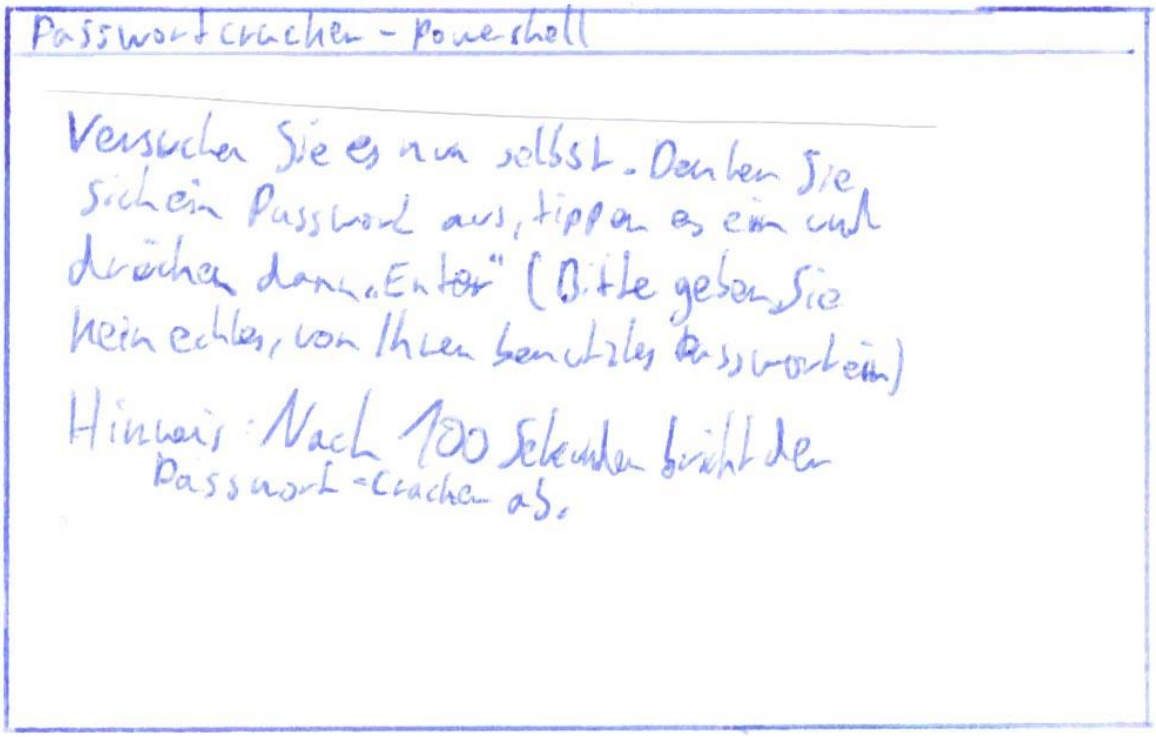
Alternativ kann z.B. über einen Klick auf einen Button der Vollbildschirm ausgelöst werden und dort der Nutzer zu weiteren Aktionen gedrängt werden.

Demonstration Passwörter



Die Demonstration zur Sicherheit von Passwörtern läuft in der Powershell/Kommandozeile ab. Diese dient quasi als Wrapper für John(the Ripper), damit dessen Passwortdateien, Optionen zu Hashverfahren, etc. unsichtbar im Hintergrund verwaltet werden können. Zuerst wird anhand eines Vorschlags demonstriert, wie schnell ein einfaches Passwort geknackt wird.





Anschließend kann der Nutzer eigene Passwörter testen. Die Versuchszeit wird hierbei beschränkt, da die Demo natürlich nur eine begrenzte Zeit laufen sollte.