Benutzer-Authentifikation

Das Ziel dieser Arbeitsblätter ist es, die Studenten in die Problematik der Benutzerauthentifikation einzuführen. Authentifikation - oder auch der Beweis, dass jemand derjenige ist, den er behauptet zu sein – ist eine der häufigsten und wichtigsten Sicherheitspraktiken, die uns im Alltag begegnen. Als Benutzer muss man seine Identität ständig beweisen, sei es entweder online (Websites), für eigene Geräte (zum Beispiel Entsperren des Smartphpones) oder fremde Geräte (wie z.B. Bankautomaten).

Die häufigste Methode der Authentifikation sind Passwörter. In diesem Modul helfen wir Schülern herauszufinden, was ein sicheres Passwort genau ist und wie man Passwörter hackt, respektive wie man sich dagegen verteidigen kann. Wir zeigen den Schülern drei Arten von Authentifikation - Besitz, Wissen und Eigenschaften – mit Aktivitäten zu Biometrie, alternativen Passwortschemen (graphische Passwörter) und Wiederherstellungsmethoden vergessener Passwörter.

Nach der Bearbeitung dieses Moduls sollten die Schüler wissen, was Authentifikation ist und wie man sich authentifiziert. Sie sollten die drei vorgestellten Möglichkeiten zur Authentifikation aufzählen, erklären und differenzieren können. Sie werden lernen, wie man sichere Passwörter wählt und sie werden sich den Risiken sowie den einfachen Gegenmaßnahmen bewusst sein. Ausserdem werden sie neue Passworttechnologien wie Biometrie und graphische Passwörter erkundet haben. Durch die Auseinandersetzung mit den wichtigsten Sicherheitsproblemen wird dieses Modul die Schüler unterstützen, eine konkretere Vorstellung von Sicherheit aufzubauen, und ihnen erlauben, sich sicherheitsbewusster in ihrem wirklichen Leben zu verhalten.

# Einführung

Einführungspräsentation Authentifikation:

* Was bedeutet es sich zu authentifizieren?
* Wie authentifizieren wir uns im echten Leben? Oder am Telefon?
* Konzept eines geteilten Geheimnisses.
* Die drei Arten der Authentifikation.

# Gute Passwörter Verwenden

In diesem Modul wirst du lernen, wie man sichere Passwörter wählt.

Gehe auf <https://howsecureismypassword.net/>

Diese Seite lässt dich die Stärke verschiedener Passwörter testen. Es gibt dir eine Schätzung, wie lange ein Angreifer benötigen würde, um ein Passwort zu erraten.

Probiere einige Passwörter aus. Wie lange dauert es jeweils bis diese Passwörter gebrochen sind?

passwort

passwort123

pässwört

geknackt

01081291

qwertzuiop

D1tt5U3

Tr0ub4dour&3

chuchichaeschtli

correcthorsebatterystaple

correct horse battery staple

n3k05uxu\_phxsym

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Versuche nun für jede der unten geforderten Regeln neue Passwörter auszusuchen. Was ist das stärkste Passwort, das du finden kannst? Welches das schwächste? (Gebe auf keinen Fall deine richtigen Passwörter ein!)

|  |  |  |
| --- | --- | --- |
| **Regel**: | **Stärkstes Passwort**: | **Schwächstes Passwort**: |
| * Höchstens 8 Zeichen | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| * Mindestens 8 Zeichen | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| * Mindestens 16 Zeichen | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| * Zwischen 8 und 16 Zeichen | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| * Mindestens 8 Zeichen ohne Wörterbuchwörter. | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| * Mindestens 8 Zeichen mit mindestens einem Kleinbuchstaben, einem Grossbuchstaben, einem Symbol, einer Zahl und ohne Wörterbuchwörter | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| * Mindestens einem Kleinbuchstaben, einem Grossbuchstaben, eine Zahl und einem Spezialzeichen:  (#,-./:=?@[]^{}~) | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| * Höchstens 32 Zeichen, keine Wörterbuchwörter länger als 4 Zeichen. | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |

Obwohl es sehr viele Passwörter mit bis zu 8 Zeichen gibt, so haben Sie zu Beginn gesehen, dass „passwort“ sofort erraten wird. Warum?

Wieso denken Sie, wird ein Passwort wie „01081291“ schnell erraten?

Ein Passwort wie „qwertzuiop“ ist kein Wort, aber wird trotzdem sehr schnell erraten. Warum?

Das Wort „ chuchichaeschtli“ is ein typisches schweizerisches Wort, aber es gilt als starkes Passwort. Wieso?

Zähle drei Eigenschaften eines starken Passworts auf.

Zähle drei Eigenschaften eines schwachen Passworts auf.

# Passwörter Knacken

In diesem Modul wirst du lernen, wie man sich in Accounts hacken kann indem man die Passwörter errät. Wir nehmen an, du versuchst dir Zugriff auf Bankaccounts zu verschaffen.

Stelle dir vor, dass du Geld von einer lokalen Bank zu stehlen versuchst. Du hast es geschafft, dir eine Liste mit den Passwörter der Accounts zu organisieren. Aber die Passwörter sind verschleiert. Aber du weisst, wie sie verschleiert wurden. Daher bist du in der Lage, die PINs zu erraten und zu gucken, ob sie mit einem der verschleierten Passwörter der Liste übereinstimmen.

Wenn du weisst, dass alle PINs aus 4 Ziffern bestehen (0 bis 9), wie viele der Passwörter der Liste kannst du erraten?

Besuche (Link auf Anfrage verfügbar) um verschiedene PINs verschleiern zu lassen und gucke, ob sie mit Passwörter deiner Liste übereinstimmen.

Hinweis: Probiere Muster auf dem Zifferneingabefeld, Daten oder einfach zu merkende Ziffernfolgen.

|  |  |  |  |
| --- | --- | --- | --- |
| **Passwort** | **PIN** | **Passwort** | **PIN** |
| ABAC |  | CEDD |  |
| ADED |  | CEEB |  |
| BBAB |  | CEEE |  |
| BCCF |  | DCBD |  |
| BEBC |  | DFFF |  |
| CAAB |  | ECDC |  |
| CBBD |  | ECEE |  |
| CBDC |  | ECFA |  |
| CBFA |  | EEAE |  |
| CCFD |  | EEFF |  |

Eine Brute-Force-Attacke nennt man das Durchprobieren aller möglichen Passwörter, meistens in einer Reihenfolge beginnend mit dem ersten möglichen Passwort (z.B. 0000) und endend mit dem letzten (z.B. 9999).

1. Was sind zwei Vorteile dieser Methode?
2. Was sind zwei Nachteile?

Eine Wörterbuchattacke (englisch: dictionary attack) dagegen probiert die am meisten genutzten Passwörter zuerst (z.B. 1234) und die unbeliebtesten zuletzt (in absteigender Reihenfolge).

1. Was sind zwei Vorteile dieser Methode?
2. Was sind zwei Nachteile?

Welche Strategie hast du benutzt um die Passwortliste zu erraten? Wie viele Passwörter konntest du erraten?

Wie viele mögliche 4 Ziffern PINs gibt es? Zeige, wie du auf deine Antwort kommst.

In dieser Übung durftest du sooft probieren, wie du wolltest. Wieso würde es nicht funktionieren, wenn du das Gleiche bei einer Log-in Seite probieren würdest?

Basierend auf deiner Erfahrung im Erraten dieser Passwörter, nenne zwei Gründe, warum das zufällige Zuweisen eines Passworts eine gute Idee sein könnte.

Denke an deine eigenen Erfahrungen mit Passwörter und zähle zwei Nachteile von zufällig zugewiesenen Passwörtern auf.

# Sicherheitsfragen (Personal Knowledge Questions)

Passwörter sind nicht die einzige Möglichkeit sich zu authentifizieren. Falls jemand sein Passwort vergessen hat, kann er oft mittels einer zusätzlichen Sicherheitsfrage seine Identität beweisen und bekommt so trotzdem Zugriff auf seinen Account. In dieser Übung werden Sie lernen, was Sicherheitsfragen sind.

Einfach gesagt sind das Fragen, die für die echte Person einfach zu beantworten sind, dies aber für alle anderen beinahe unmöglich sein sollte. Die Wahl der genauen Frage kann aber zu Problemen führen. In dieser Übung werden Sie versuchen entsprechende Antworten für Accounts von berühmten Personen zu erraten, indem Sie lediglich Internetsuchen für die Antworten benützen.

|  |  |
| --- | --- |
| **Xherdan Shaqiri** |  |
| Was ist der ledige Name Ihrer Mutter? |  |
| Was ist Ihre Lieblingsfarbe? |  |
| In welcher Stadt wurden Sie geboren? |  |
| Was war Ihre erste Telefonnummer? |  |
| Was ist Ihr Lieblingssport? |  |
|  |  |
| **Justin Bieber** |  |
| Was ist der ledige Name Ihrer Mutter? |  |
| Was ist Ihre Lieblingsfarbe? |  |
| In welcher Stadt wurden Sie geboren? |  |
| Was war Ihre erste Telefonnummer? |  |
| Was ist Ihr Liebslingssportteam? |  |
|  |  |
| **Ariana Grande** |  |
| Was ist der ledige Name Ihrer Mutter? |  |
| Was ist Ihre Lieblingsfarbe? |  |
| In welcher Stadt wurden Sie geboren? |  |
| Was war Ihre erste Telefonnummer? |  |
| Was ist Ihr Lieblingsbuch? |  |
|  |  |
| **Rihanna** |  |
| Was ist der ledige Name Ihrer Mutter? |  |
| Was ist Ihre Lieblingsfarbe? |  |
| In welcher Stadt wurden Sie geboren? |  |
| Was war Ihre erste Telefonnummer? |  |
| Was ist Ihr Libelingsschauspieler? |  |
|  |  |
| **Roger Federer** |  |
| Was ist der ledige Name Ihrer Mutter? |  |
| Was ist Ihre Lieblingsfarbe? |  |
| In welcher Stadt wurden Sie geboren? |  |
| Was war Ihre erste Telefonnummer? |  |
| Was ist der Name Ihres ersten Kindes? |  |

Welche dieser Fragen ist die sicherste? Warum?

Welche ist die unsicherste? Wieso?

Ist es eine gute Idee persönliche Informationen zur Authentifizierung zu benützen? Warum oder warum nicht?

Wenn jetzt ein Freund von Ihnen probieren würde ihre Sicherheitsfragen zu beantworten, könnte er die Antworten mittels Google finden? Über welche anderen Informationsquellen könnte er verfügen, um sich Zutritt zu Ihren Accounts zu verschaffen?

Sind Sicherheitsfragen der einzige Weg um ein vergessenes Passwort zurück zu setzen? Welche anderen Methoden könnten besser sein? Warum?

In dieser Übung haben Sie sich Zutritt zu Accounts durch das Erraten der Sicherheitsfragen des Passworts-Wiederherstellen-Mechanismus verschafft. Basieren auf dem was Sie hier gelernt haben: ist es eine gute Idee persönliche Informationen in den Passwortvorgang einzubeziehen? Wieso oder wieso nicht?

# 

# Graphische Passwörter

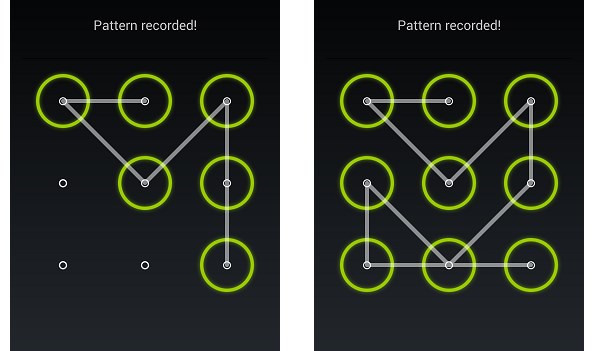
Obwohl die meisten Passwörter denen wir begegnen nur aus Text bestehen, gibt es doch noch andere Arten. Graphische Passwörter benutzen nicht Text sondern Bilder um Benutzer das Einlogen zu erleichtern und natürlich gibt es auch hier viele verschiedene Arten und Ansätze.

In dieser Übung werden Sie verschiedene Arten von graphischen Passwörter ausprobieren, lernen wie diese funktionieren und ihre Merkbarkeit ermitteln.

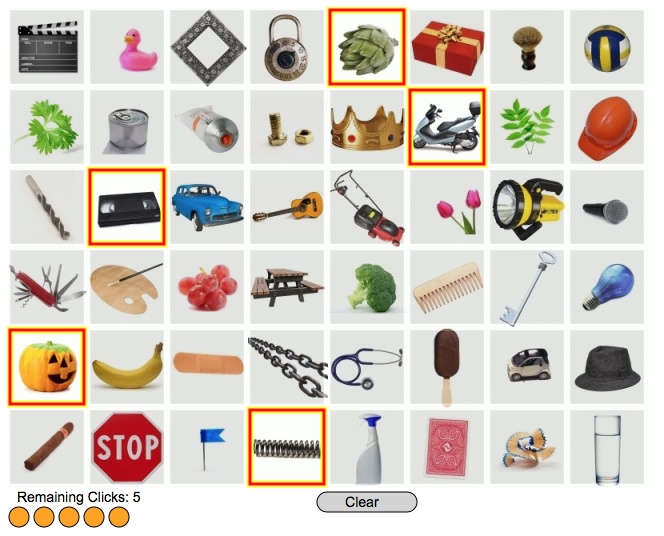
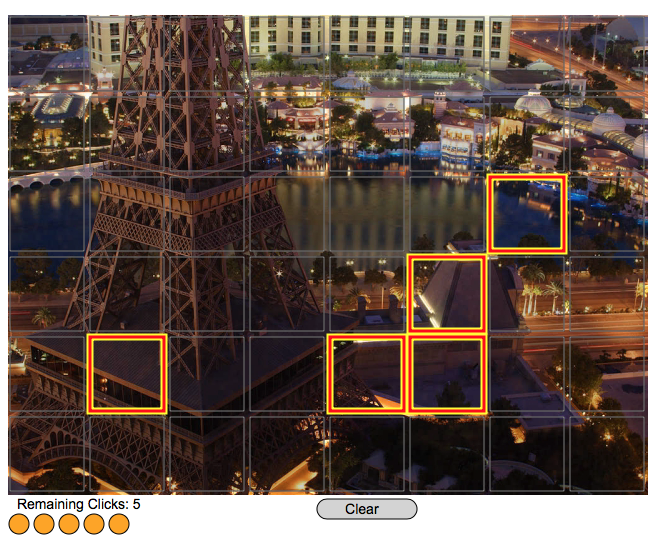
### Android Muster Sperre (auf einem Android-Smartphone)

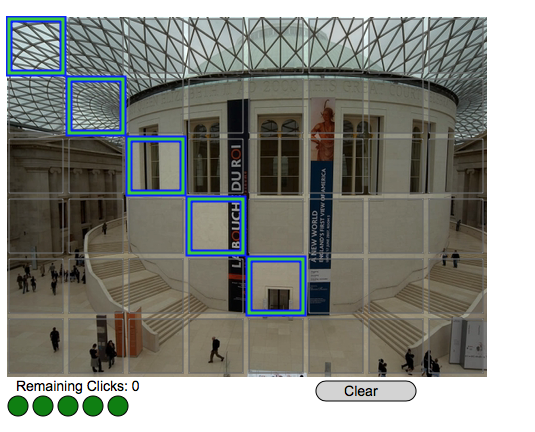
Die Android Muster Sperre ist ein graphisches Passwort auf Android-Smartphones, welches als Bildschirmsperre benutzt werden kann. Sie besteht aus einem Gitter, dessen Punkte man zu einem Muster verbinden kann, und um sich einzuloggen muss diese Zeichnung wiederholt werden (Die Gitterpunkte müssen in der selben Reihenfolge berührt werden).

Gehen Sie auf dem Android-Smartphone in die App-Auswahl und von dort in das Einstellungsmenü. Scrollen Sie runter und gehen Sie in das Sicherheitsmenü, wählen sie Bildschirmsperre und setzen Sie es auf Muster. Wählen und bestätigen Sie ein Musterpasswort und sperren Sie danach das Telefon. Geben Sie Acht, dass Sie das Muster nicht vergessen!



### PassTiles (Zuweisung, Benutzerwahl, Objekte)





PassTiles ist ein graphisches Passwortsystem, in welchem die Passwörter aus einer vom Benutzer gewählten Menge von Quadraten eines Gitters bestehen. Um sich einzuloggen muss man die 5 Quadrate auswählen, aus denen das eigene Passwort besteht. Die Reihenfolge ist nicht wichtig.

Es gibt drei Variationen von PassTiles:

a) Bei Image PassTiles weist das System dem Benutzer fünf Quadrate zu. Dieser muss sich deren Position im Gitter mithilfe des darunter liegenden Bildes merken. Die Reihenfolge ist dabei nicht wichtig.

b) Chosen PassTiles funktioniert genau gleich wie Image PassTiles, aber anstatt ein vom System zugewiesenes Passwort zu erhalten, darf der Benutzer es sich selbst aussuchen.

c) Bei Object PassTiles weist das System dem Benutzer fünf Objekte als Passwort zu, die bei jedem Login an anderen Positionen erscheinen. Um sich ein zu logen muss der Benutzer die richtigen Objekte anwählen.

Gehen Sie auf (Link verfügbar auf Anfrage)

Wählen Sie einen Benutzernamen und stellen Sie sicher, dass Sie nicht den selben Benutzernamen wie eine andere Person auswählen. Probieren Sie alle drei Systeme aus (IPA, IPU und OPA)

Tippen Sie den Benutzernamen ein und drücken Sie „Create“ um zu beginnen. Folgen Sie den Instruktionen um ein Passwort zu erstellen, auszuprobieren und schliesslich zu bestätigen. Folgen Sie dem Link, falls Sie Hilfe benötigen.

|  |  |  |
| --- | --- | --- |
| Image PassTiles | Chosen PassTiles | Object PassTiles |
| IPA\_1 | IPU\_1 | OPA\_1 |
| IPA\_2 | IPU\_2 | OPA\_2 |
| IPA\_3 | IPU\_3 | OPA\_3 |

Wie finden Sie diese Passwörter verglichen mit den Textpasswörtern? Denken Sie, dass Sie sich an die graphischen Passwörter erinnern könnten, wenn Sie sie im richtigen Leben benutzen würden?

Wenn Sie einen Bekannten beim Einlogen zusehen würden, wäre es für Sie einfacher oder schwieriger, sich an das Passwort zu erinnern?

Bei der Android Muster Sperre, denken Sie, Sie könnten das graphische Passwort eines anderen Benutzers herausfinden, indem Sie nur auf den Bildschirm schauen?

Probieren Sie es aus: Lassen Sie einen Freund das Telefon mehrmals entsperren (ohne dass Sie zusehen) und probieren Sie dann das Passwort zu erraten. Falls es nicht gelingt, soll er oder sie die „Fingerspuren“ auf dem Glass nochmals nachziehen. Können Sie es korrekt nachziehen?

War es einfacher oder schwieriger sich an die Objekt Bilder zu erinnern verglichen mit den Hintergrundbildern? Welche Methode wäre Ihrer Meinung nach besser als Passwort geeignet.

Als Sie und Ihre Gruppenmitglieder Ihre eigenen PassTiles Passwörter gewählt haben, haben Sie teilweise die selben Quadrate ausgewählt? Warum ist es sicherer, diese Quadrate automatisch zuzuweisen?

Wie viele mögliche Passwörter gibt es für die PassTiles Methode, wenn die Reihenfolge keine Rolle spielt? Erklären Sie, wie Sie es berechnet haben.

Sind diese Passwörter sicherer oder unsicherer als Textpasswörter? Wieso?

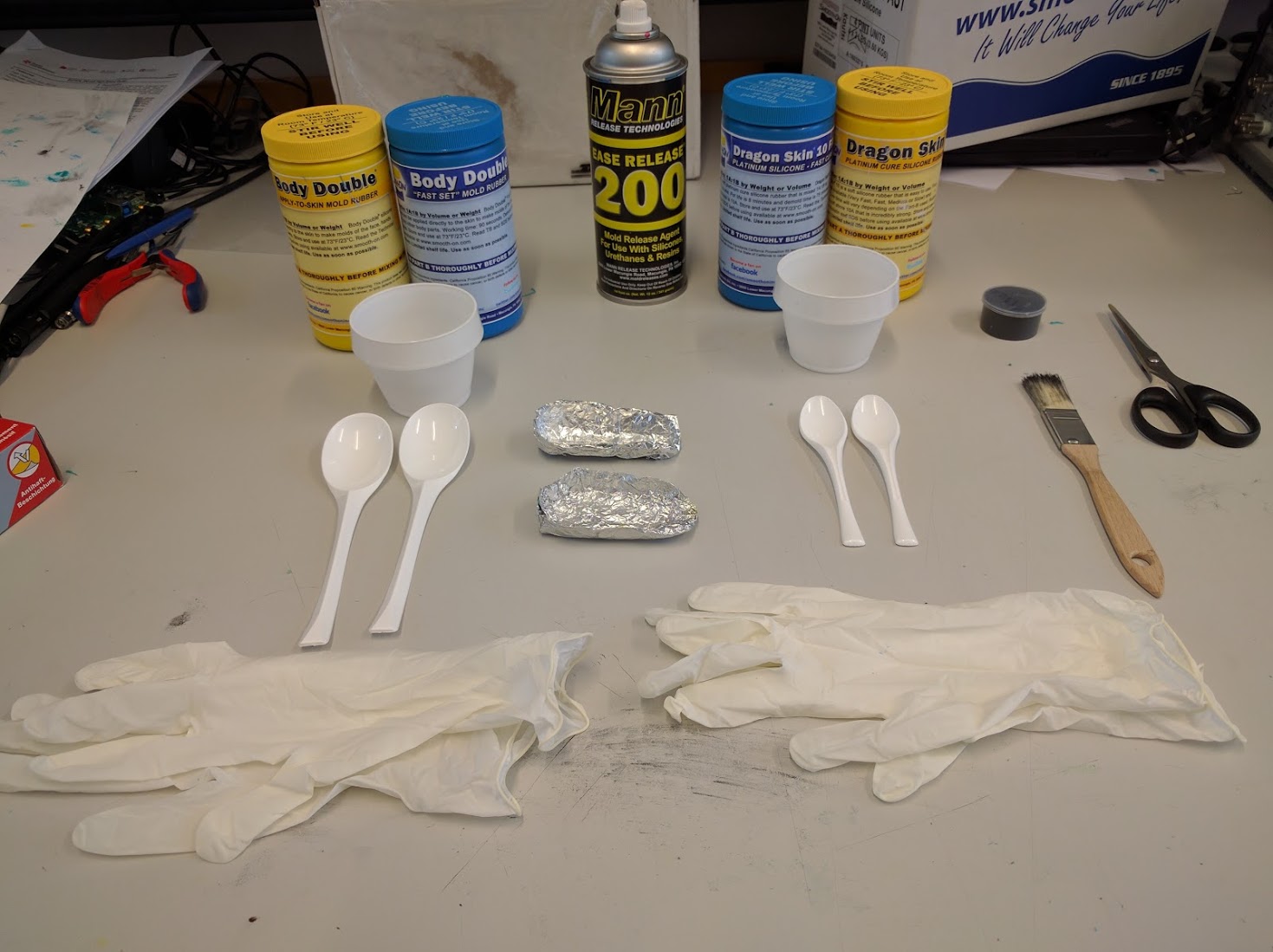
# Biometrie

Man kann sich auch authentifizieren, indem man ein eindeutiges Merkmal der zu authentifizierenden Person überprüft. Diese eindeutigen Merkmale des Körpers werden *Biometrie* genannt. Am häufigsten wird heutzutage der Fingerabdruck benutzt. Aber auch Scans der Iris, die Form der Ohren oder das Verlaufsmuster der Venen in den Händen können benutzt werden, um eine Person eindeutig zu identifizieren.

Im ersten Teil dieses Moduls wirst du einen Abdruck deines eigenen Fingers anfertigen und versuchen, damit dein Smartphone zu entsperren. Falls du kein Telefon mit einem Fingerabdrucksensor besitzen, darfst du es an einem der Vorführungsmodelle probieren.

Im zweiten Teil wirst du lernen, wie man Fingerabdrücke von alltäglichen Oberflächen kopieren kann.

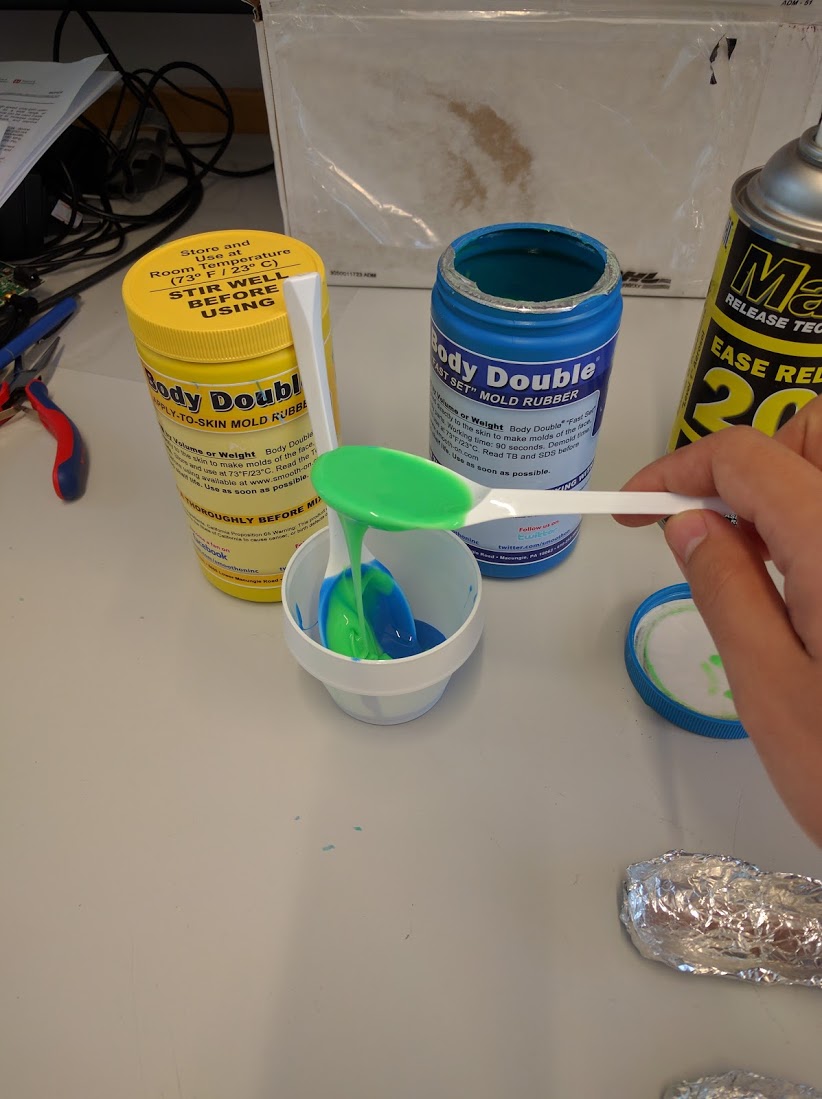
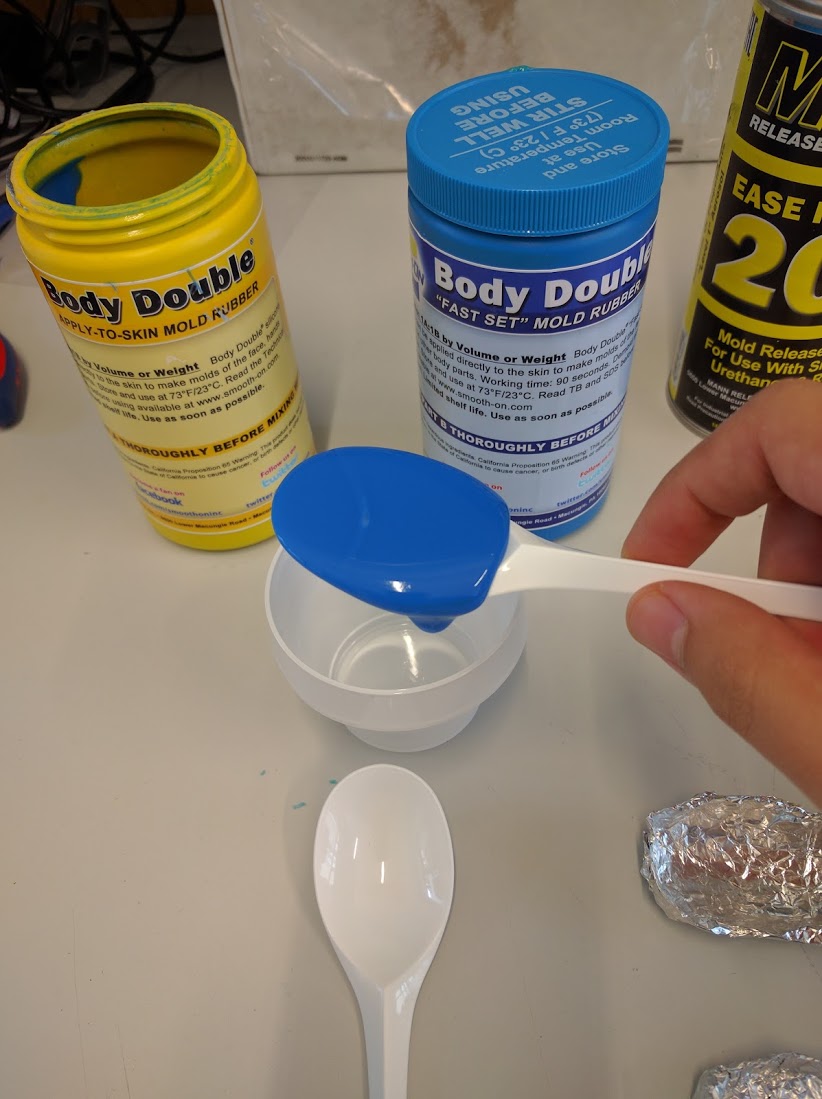
Materialien



Hier ist eine Liste der Materialien, die du benötigen wirst: Auf der linken Seite siehst du die Utensilien um die Abdrucksform zu erstellen („Body Double“), worin die Fingerkopie danach erstellt werden kann: Einen Plastikbecher und zwei grosse Löffel um die Mischung anzurühren. In der Mitte siehst du zwei Schälchen aus Aluminiumfolie um darin den Abdruck zu erstellen. Auf der rechten Seite siehst du den Silikon („Dragon Skin“) woraus dann die Kopie des Fingers erstellt wird, sowie einen weiteren Mixbecher und zwei kleinerer Löffel. Die Aluminiumbehälter wirst du selbst rollen.

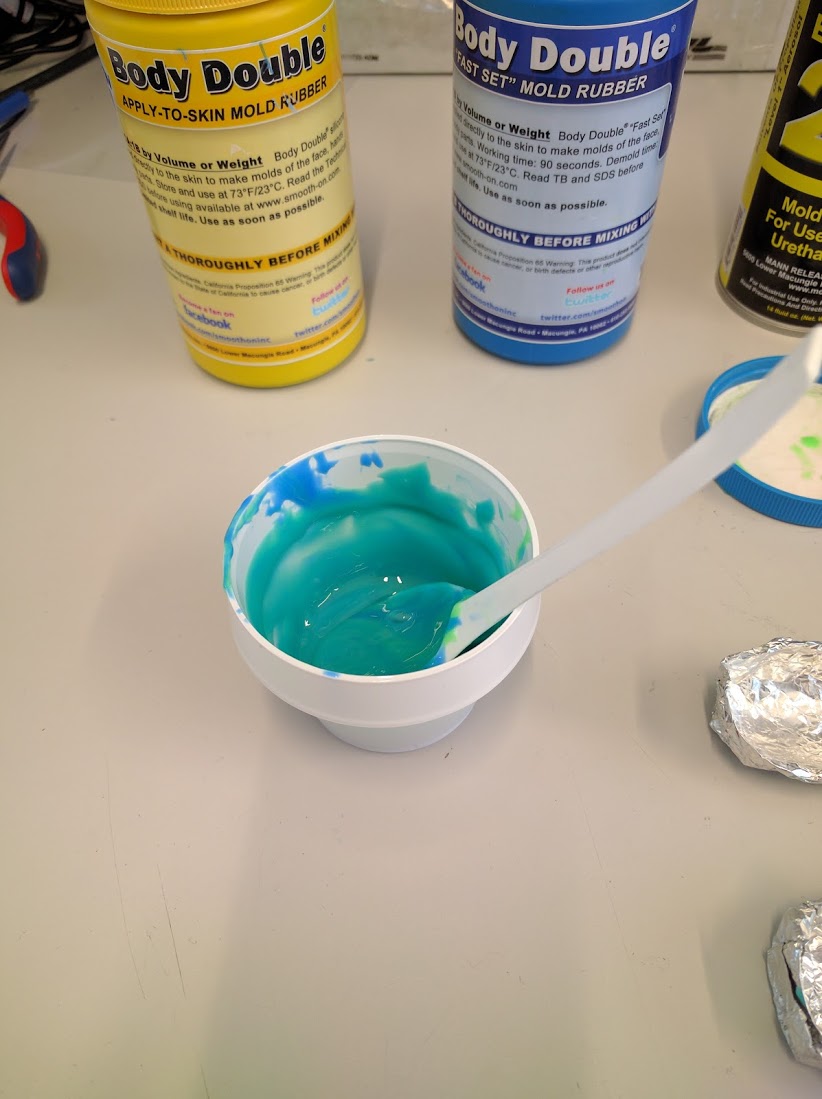
Bevor du beginnst, solltest du zuerst alle Schmuckstücke von deinen Händen entfernen (Ringe, Armbänder, etc.) und falls du ein altes T-Shirt oder einen Schurz mitgebracht hast, ziehe es besser an, da die ganze Sache etwas schmutzig werden kann.

## Schritt 1



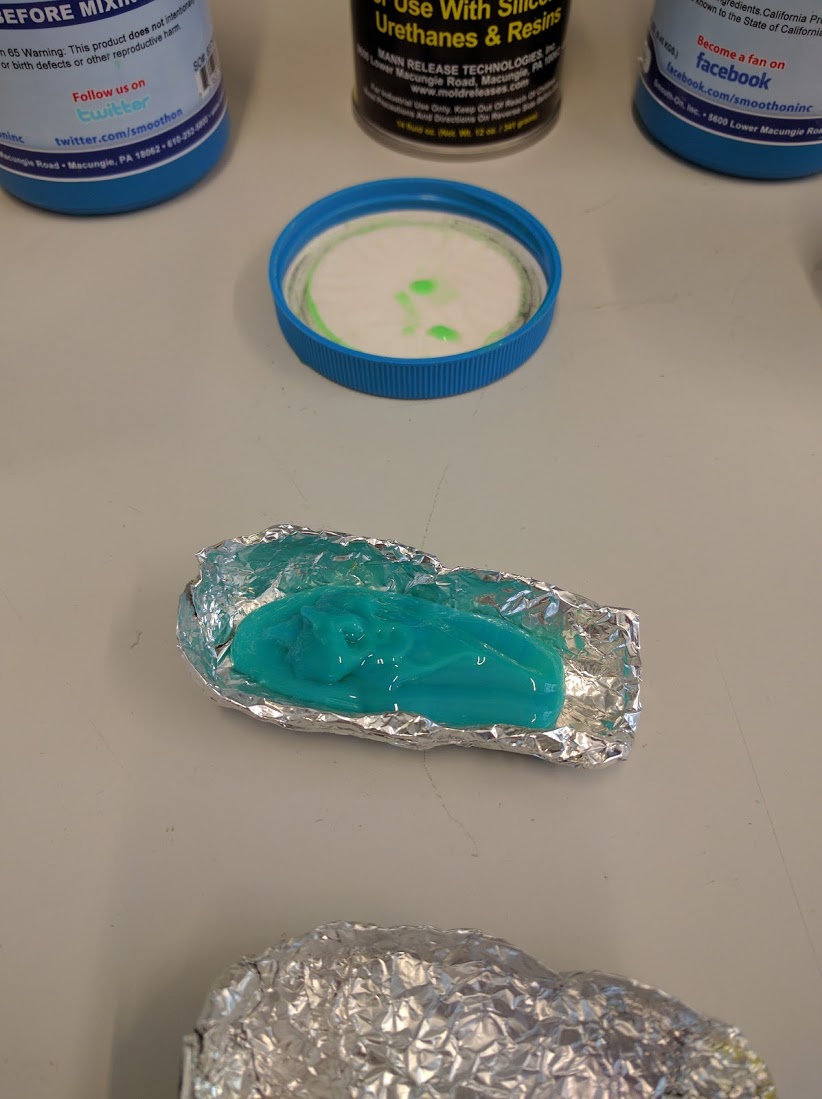
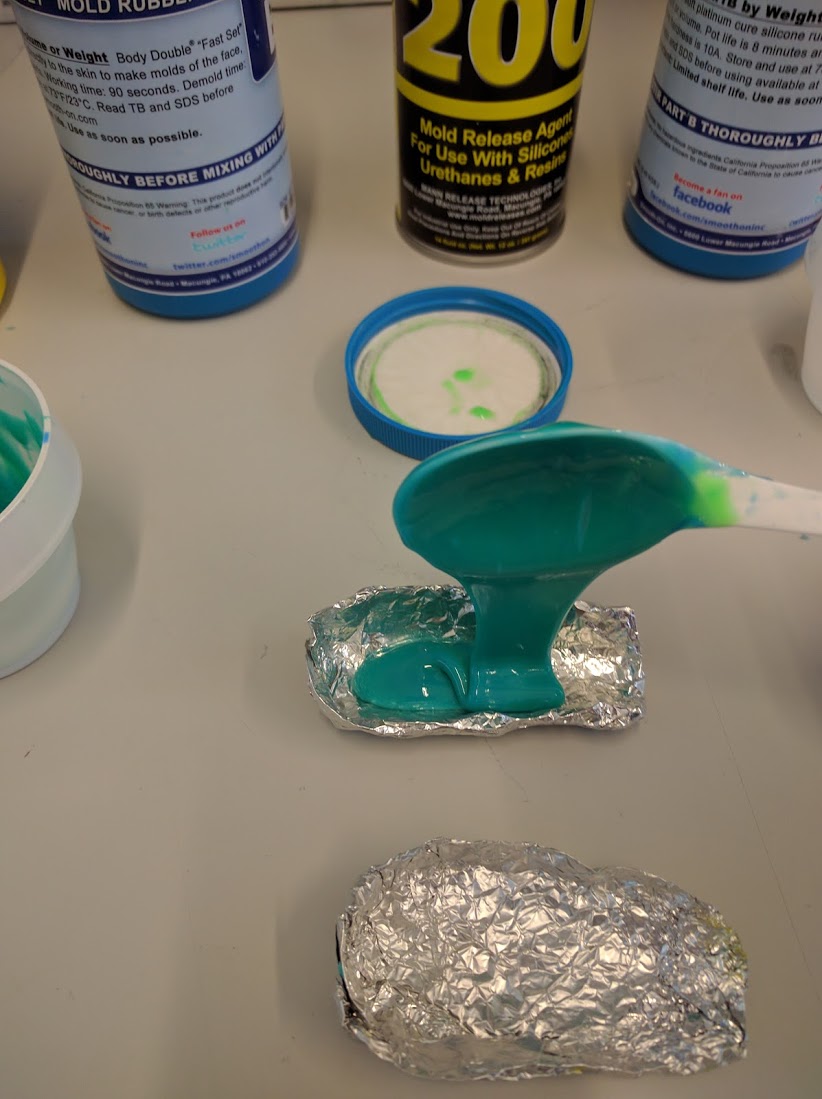
Nimm den Plastikbecher und zwei saubere **GROSSE Plastiklöffel.** Benutze jeweils einen separaten Löffel, um einen vollen Löffel des blauen **Body Double**  und einen vollen Löffel des grünen **Body Double** in einen der Plastikbecher zu tun.

**WICHTIG: Benutze NICHT den gleichen Löffel für beide Komponenten. Stelle sicher, dass du beide Flüssigkeiten jeweils mit einem neuen und sauberen Löffel schöpfen.**



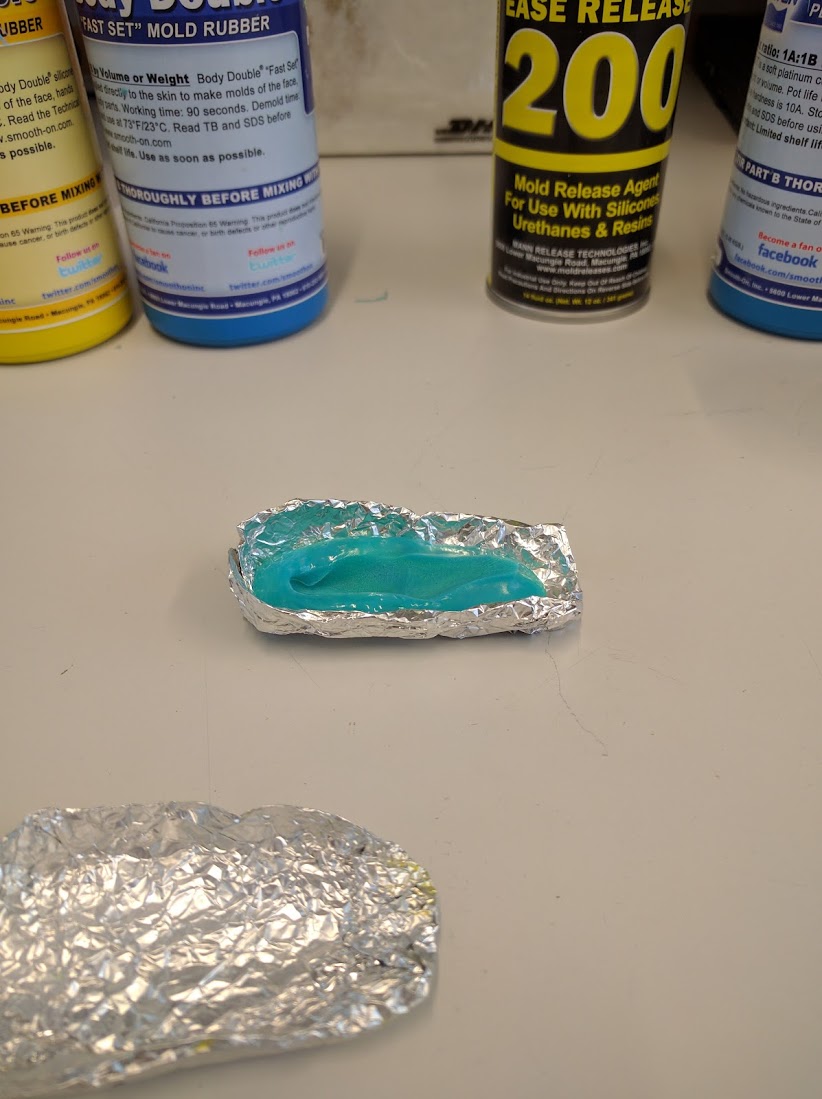
Mische die zwei Substanzen vorsichtig. Versuche, keine Luftblasen zu erzeugen. Das Bild zeigt die fertige Mischung, wenn sie gut verrührt wurde.

## Schritt 2



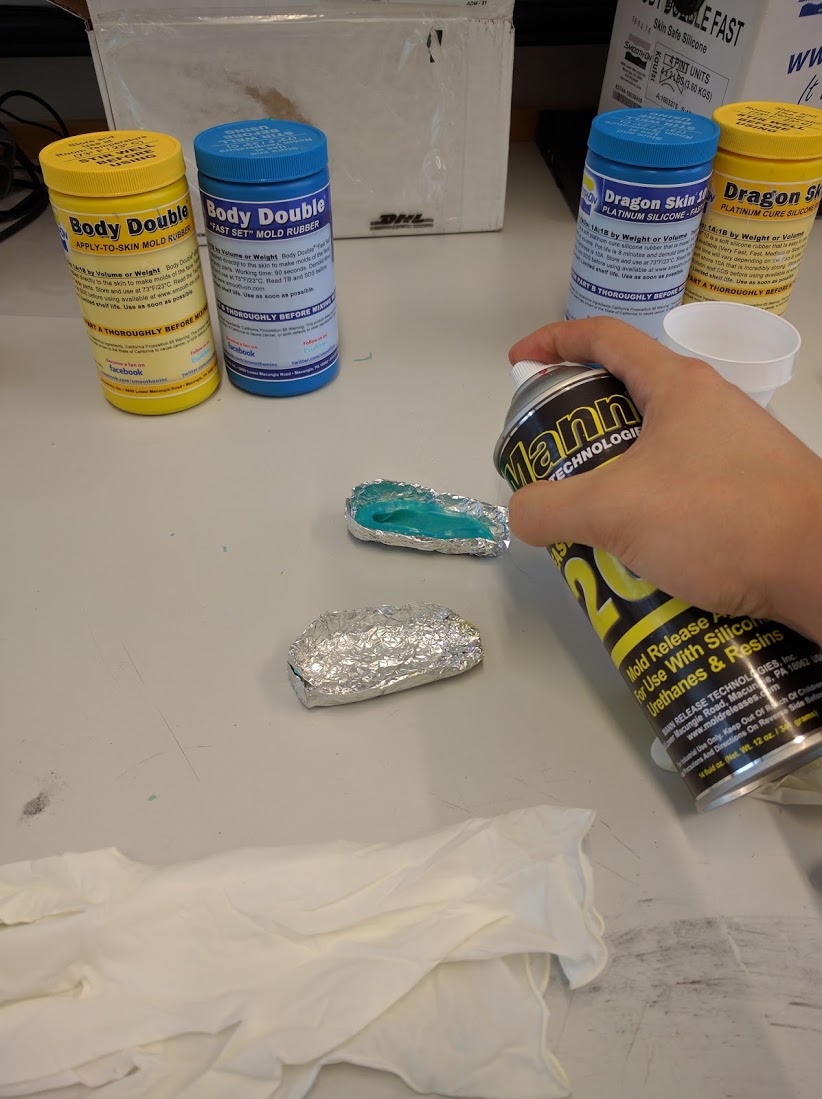
Benutze den grossen Löffel, um einen vollen Löffel in die Aluminiumfolie zu giessen. Drücke danach den Finger mit dem du normalerweise Ihr Telefon entsperrst leicht in die Mischung. Drücke nicht zu fest und versuche, deinen Finger für 7-8 Minuten nicht zubewegen, damit der Fingerabdruck nicht verzerrt wird.

## Schritt 3



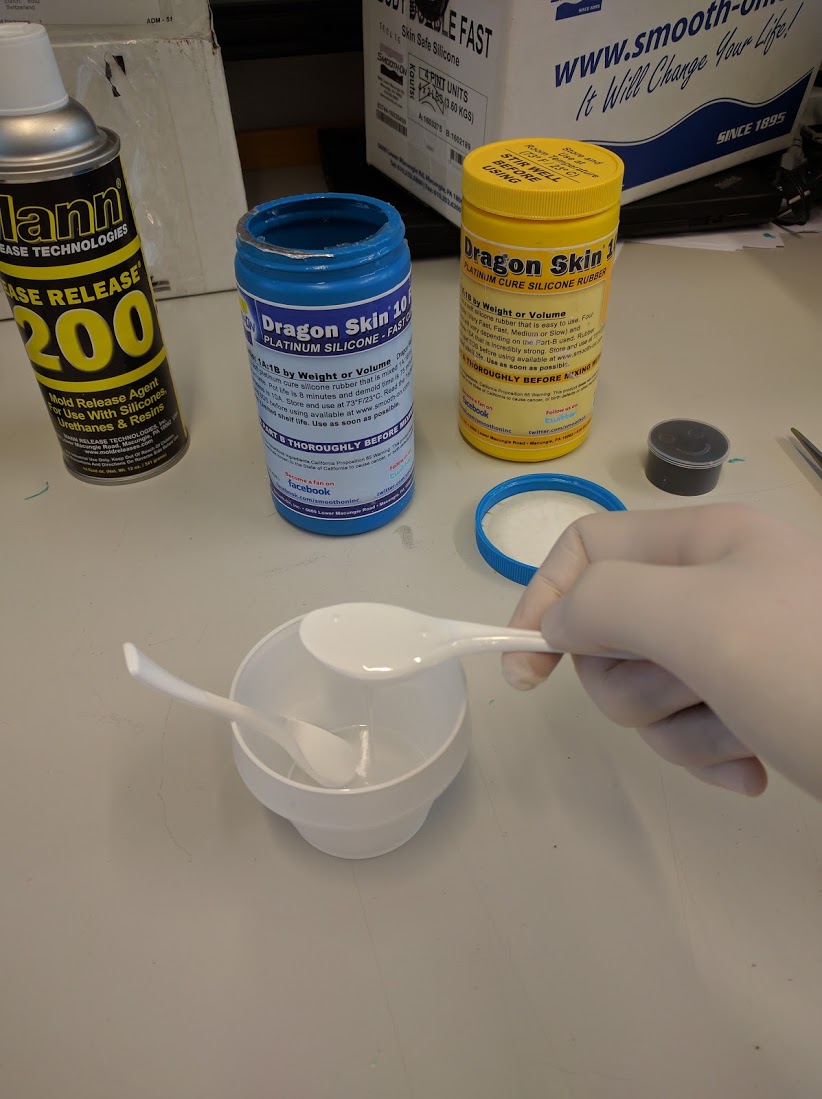
Entferne nach 10 Minuten deinen Finger vorsichtig von nun ausgehärteten Mischung.

## Schritt 4



Um sicher zu stellen, dass du später den Abdruck von der Abdrucksform entfernen kannst, sprühe den **„Ease-Release“-Spray** zwei Mal für je eine Sekunde in die Form. Stelle sicher, dass du die Innenseite der Form gut erwisc, damit sich der Silikonabdruck später auch gut loslösen lässt.

## Schritt 5



Für den nächsten Schritt wirst du die Komponenten der **„Dragon Skin“** mischen, um damit den Silikon zu erzeugen. Ziehe die Handschuhe an, da der Silikon ziemlich klebrig ist. Nimm den zweiten, **sauberen Plastikbecher** und die **zwei kleinen Plastiklöffel.** Fülle jeweils einen separaten Löffel von beiden Komponenten (beide Komponenten sind weiss) in den Becher und mische sie gut. Daraus erstellst du deine Fingerkopie.

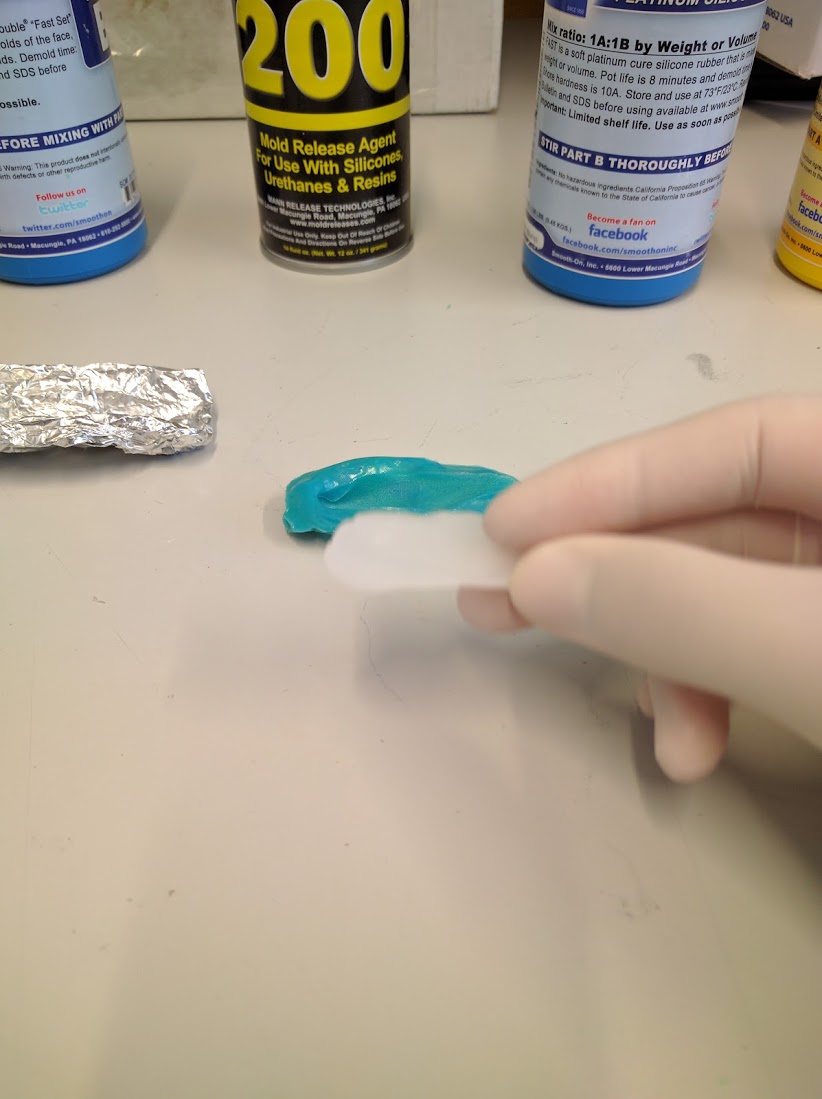
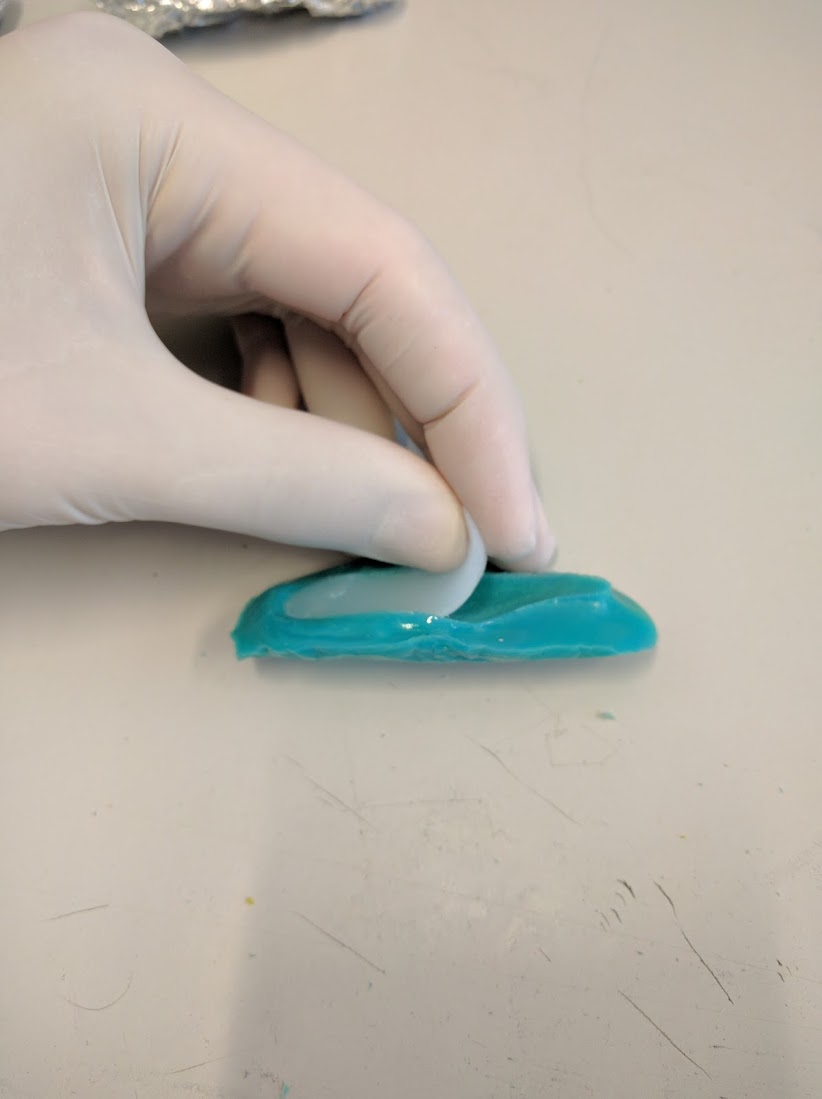
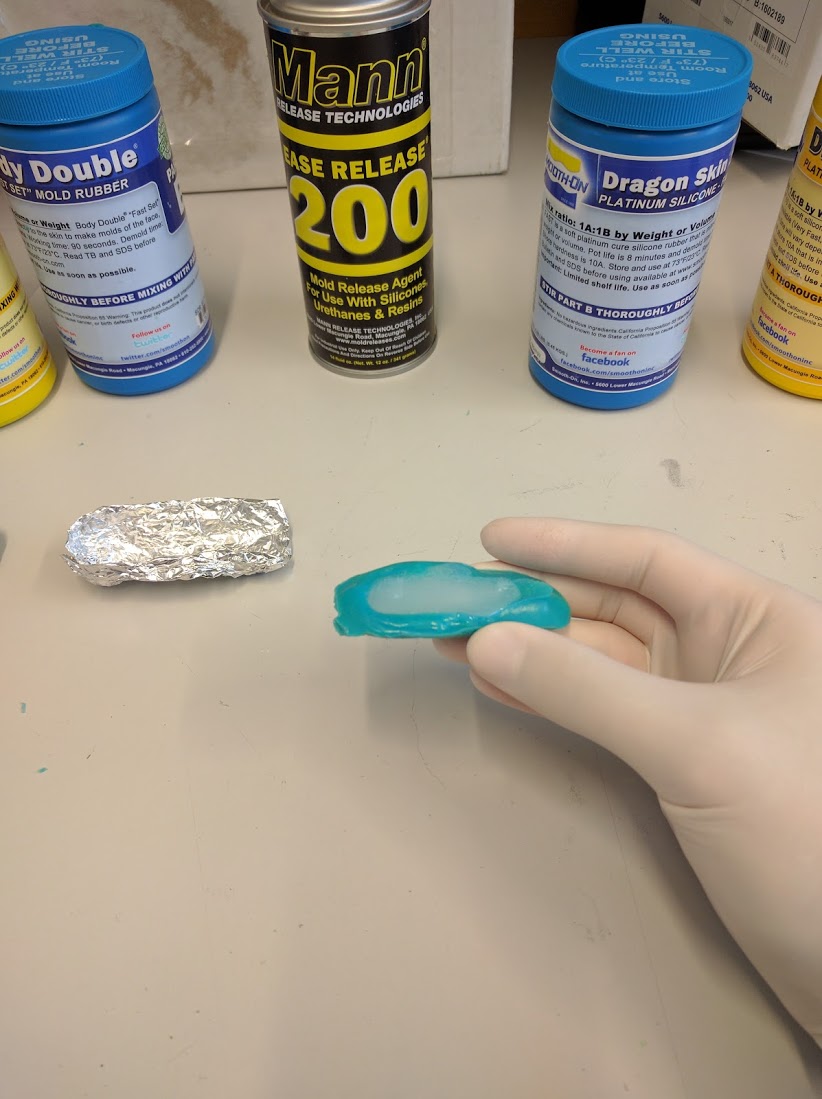
**WICHTIG: Benutze NICHT den selben Löffel für beide Komponenten. Stelle sicher, dass du jede der Zutaten mit einem neuen, sauberen Löffel nimmst.**

Schritt 6



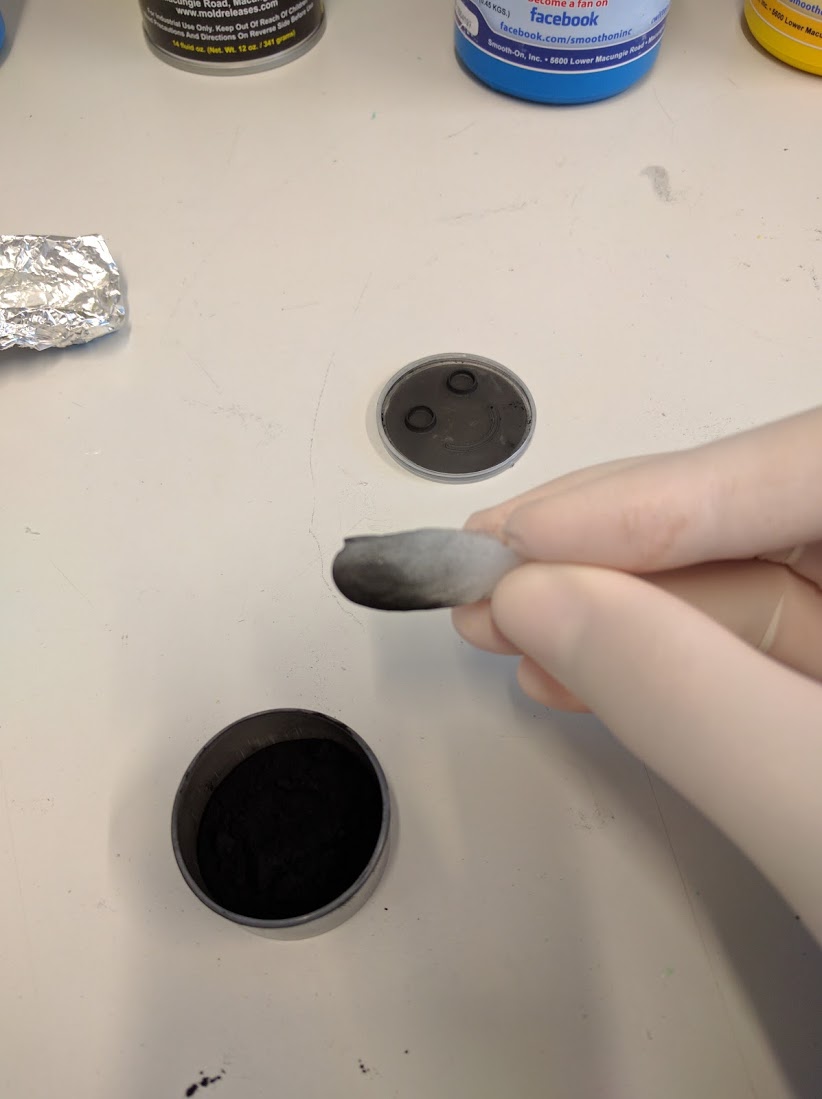
Wenn du die zwei Komponenten gut verrührt hast, giesse vorsichtig einen Löffel voll über die zuvor erstellte Abdrucksform. Wenn du Luftbläschen siehst, stupse die Form vorsichtig an, um sie aufsteigen zu lassen. Platziere die Form auf einem Stück Papier und **schreibe deinen Namen darauf.** Lasse den Silikon nun trocknen.

## Schritt 7



Wenn der Silikon ausgehärtet ist, kannst du ihn vorsichtig aus der Form entfernen. Du hast jetzt eine Kopie deines Fingers aus Silikon!

## Schritt 8

Moment kannst du den Abdruck noch nicht zum Entsperren benutzen, da der Fingerabdrucksensor die elektrische Leitfähigkeit des Fingers prüft. Und Silikon leitet nicht. Nimm daher die Fingerkopie und tunke sie vorsichtig in ein wenig Graphitpulver. Verteile danach das Pulver mithilfe des Pinsels gleichmässig über dem Finger.

Versuche nun, das Telefon zu entsperren. Funktioniert es?

Wenn du mit diesem Modul fertig bist, kannst du die Kopie des Fingers als Andenken behalten. Aber stellen sicher, dass du ihn zerstört hast, sodass niemand ihn stehlen kann und damit dein Telefon entsperren könnte. Schneide am Ende dieser Übung mit einer Schere einen kleinen Schnitt in die Spitze des Abdrucks.

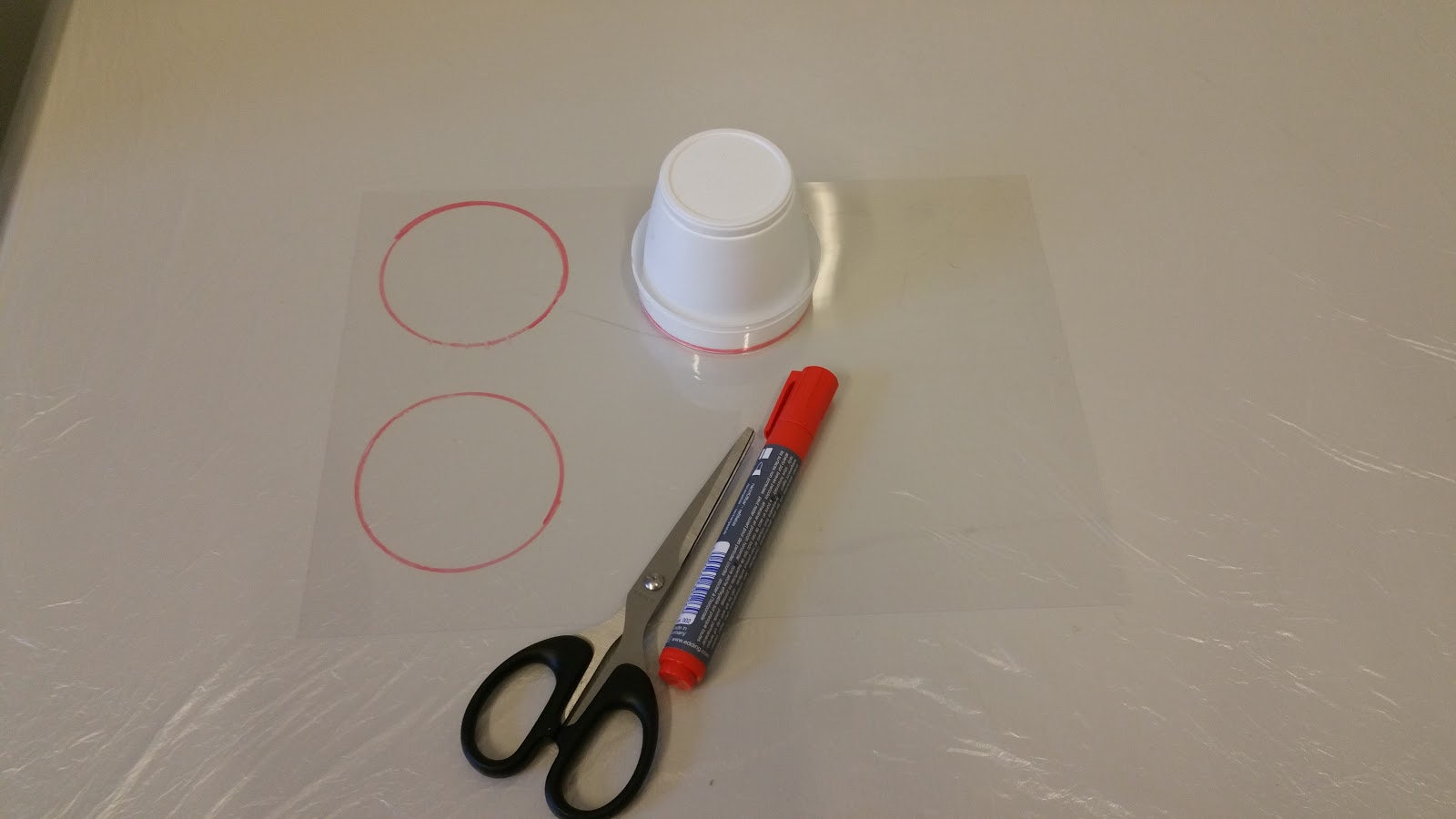
## Aktivität 2

## Authentifizierung durch Fingerabdrücke ist simpel und intuitiv. Aber unsere Fingerabdrücke sind längst nicht so ein Geheimnis, wie es erscheinen könnte. In dieser Übung wirst du lernen, wie einfach man Kopien unserer Fingernabdrücke von fast allen Oberflächen erstellen kann.

## Diese Kopie wäre für einen Angreifer der erste Schritt, falls er versuchen wollen würde, sich zu einem Benutzerkonto per Fingerabdruckleser Zutritt zu verschaffen.

Schritt 1

Die besten Abdrücke erhält man von glatten Oberflächen. Daher werden wir eine Plastikfolie benützen.

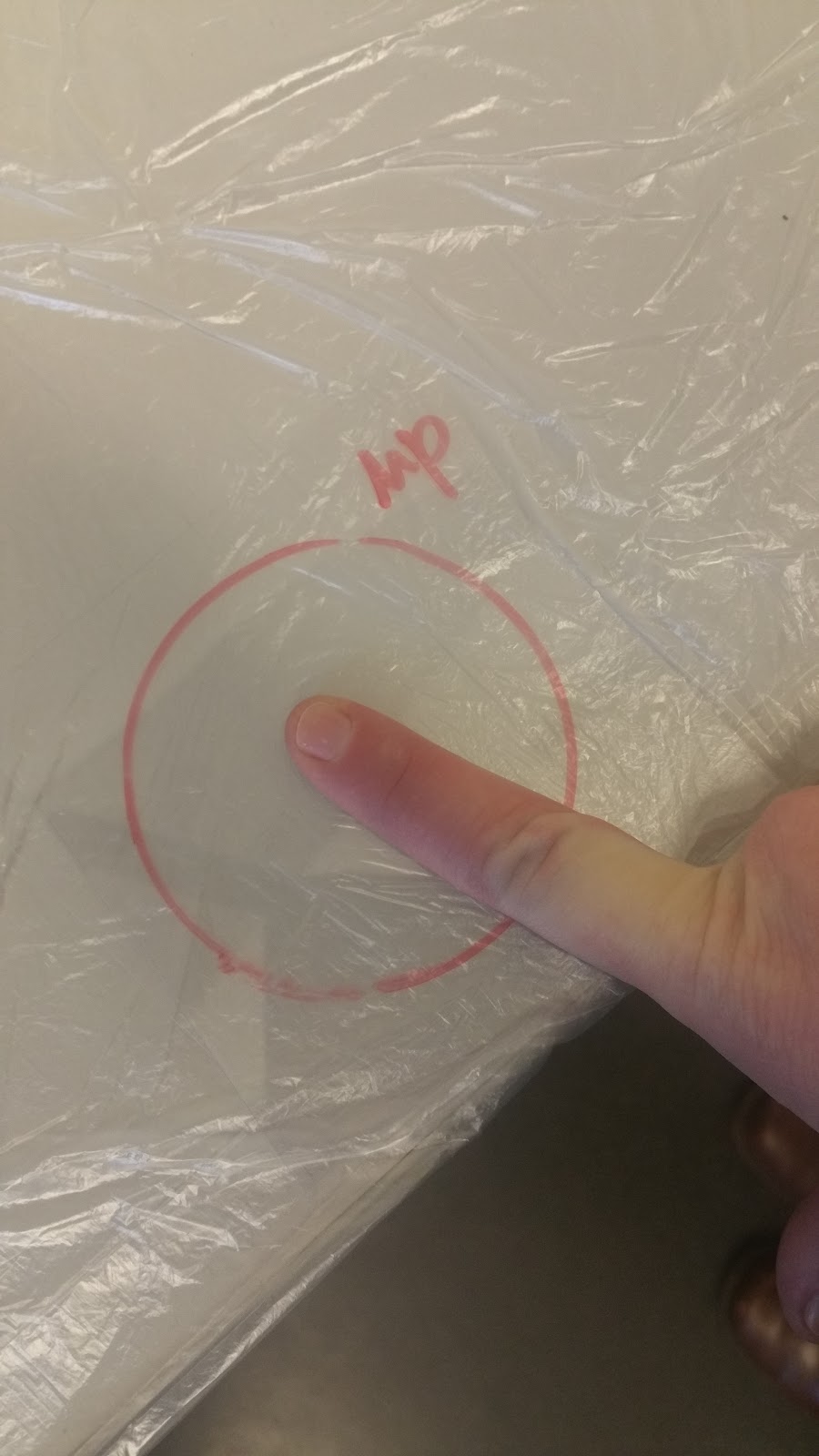


Platziere als erstes einen Becher auf der Folie und ziehe einen Kreis um den Becher. Schneide danach die Folie in quadratische Stücke, sodass sie komplett über den Plastikbecher passen und die ganze Öffnung bedecken.



Stelle sicher, dass 1) der Becher, 2) die Folie und 3) der Sekundenkleber bereit ist.

Schritt 2



Nimm deinen Finger und reibe ihn ein wenig an deiner Stirn, sodass er fettig genug für einen guten Abdruck ist. Drücke den Finger danach in das Zentrum des roten Kreises um einen Abdruck zu erzeugen. Gib Acht, dass du ihn nur ein mal drauf drückst und dass du den Abdruck nicht verschmierst. Ansonsten wiederhole den Vorgang.

Schritt 3

Öffne den Sekundenkleber, tröpfle ein wenig auf den Boden des Bechers und decke die Öffnung des Bechers mit der Folie mit deinem Abdruck darauf ab.

**Stelle sicher, dass der Abdruck auf der Unterseite der Folie ist. Also dass er Richtung Kleber zeigt!**

Warte 10 Minuten, sodass der Kleber verdampfen kann und den Fingerabdruck besser sichtbar macht.

Schritt 4



Gratulation! Du solltest jetzt einen gut sichtbaren und vor allem fixierten Abdruck deines Fingers besitzen!

Warst du in der Lage, dein Telefon mit der Fingerkopie zu entsperren? Falls nicht, was denkst du ging schief?

Was sind drei Vorteile der biometrischen Authentifizierung?

In einem System, welches Fingerabdrücke zur Authentifizierung verwendet, wie könnte Sie Ihr „Passwort“ ändern? Gibt es eine unlimitierte Anzahl an möglichen Passwörtern?

Können Sie sich etwaige Probleme mit der Privatsphäre vorstellen, wenn man Fingerabdrücke zur Authentifizierung verwendet? Ist es eine gute Idee Fingerabdrücke zur Authentifizierung auf einem System zu benutzen, auf dem man unbekannt bleiben will?

Basierend auf dieser Übung, denken Sie es ist eine gute Idee, Fingerabdrücke zum entsperren Ihres Telefons zu benutzen? Denken Sie Fingerabdrücke eignen sich, um eine zuverlässige Authentifizierung in einer Hochsicherheitsumgebung wie zum Beispiel bei einem Bank-Account zu gewährleisten?