PASSWÖRTER

Passwörter dienen dazu, eure Daten zu schützen. Sie schützen eure Emails vor unbefugtem Zugriff, sie schützen eure Dateien auf dem Computer, sie schützen eure Festplatte davor, von den Repressionsbehörden entschlüsselt zu werden. Passwörter schützen euch, sie schützen eure FreundInnen und sie schützen unsere Zusammenhänge! Dieser ganze Schutz wird zunichte gemacht, wenn ihr mit den Passwörtern nicht verantwortungsbewusst umgeht:

Passwörter sollen, so wie wir alle, einmalig sein!

Die grösste Gefahr für Passwörter ist, wenn sie wiederverwendet werden. Das sollte niemals! vorkommen. Durch das Wiederverwenden von Passwörtern gefährdet ihr dann nicht nur eine Gruppe sondern gleich mehrere Kollektive in der Szene. Jeder Login hat sein eigenes Passwort verdient.

Passwörter müssen schwer erratbar sein! Sie müssen lang & komplex sein!

Früher sind immer 8 Zeichen bei Passwörtern empfohlen worden. Mittlerweile gilt jedoch schon alles unter 12 Zeichen als zu kurz! Doch je mehr desto besser. Wenn ihr die Passwörter immer wieder übt, dann könnt ihr auch ohne Probleme mehrere 20 Zeichen lange Passwörter haben, die ihr genauso schnell tippen könnt. Die Länge des Passworts ist für die Widerstandsfähigkeit wichtiger als die Komplexität- sofern es keine simplen langen Wörter sind. Passwörter sollen auf keinen Fall in einem Wörterbuch drin stehen. Egal was für ein Wörterbuch das ist. Es gibt alle nur vorstellbaren Wörterbücher digital & es gibt Programme, die darauf zugreifen können und in Windeseile Wort für Wort ausprobieren (das nennt sich übrigens 'Brute Force' Methode / Methode der rohen Gewalt, weil einfach auf gut Glück durchprobiert wird).
Passwörter sollen Gross- und Kleinschreibung, Ziffern und Sonderzeichen enthalten. Schöpft eure Möglichkeiten aus, seid kreativ! Und: Es sollten keine Begriffe oder Namen verwendet werden, von denen andere Personen wissen oder die sich aus dem Kontext eures persönlichen Hintergrunds ergeben könnten.

Passwörter werden nicht (unverschlüsselt) aufgeschrieben!

Passwörter werden nicht (unverschlüsselt) aufgeschrieben. Auf keinen Fall. Passwörter sind nur an zwei Plätzen gut aufgehoben und die sind euer Hirn oder ein Passwortsafe. Passwörter haben nichts auf Zetteln auf eurem Schreibtisch zu tun, sie sollen nicht auf Post-Its an eurem Bildschirm kleben. Sie sollen auch nicht in unverschlüsselten Dateien auf eurem Computer abgespeichert sein. Und natürlich sollen sie auch nicht per Email, SMS oder Chat verschickt oder in Webforen über private Nachrichten ausgetauscht werden.
Wenn ihr in einer Gruppe ein gemeinsames Passwort suchen wollt, dann zerstört bitte danach den Zettel, von dem es alle auswendig gelernt haben. Noch besser ist es natürlich, das Passwort überhaupt nur über Sprache auszumachen. Prinzipiell gilt natürlich, dass Gruppenpasswörter tunlichst vermieden werden sollen.
Wenn ihr euch ein Passwort nicht merken könnt, dann übt es. Tippt es immer wieder auf einer Tastatur (am besten vorher abstecken) bis ihr es blind tippen könnt. Das Passwort ist dann nicht mehr eine Reihenfolge von Buchstaben, sondern eine Bewegung eurer Finger, die automatisch passiert (das Problem ist dann nur, wenn mensch vor einem anderen Tastaturbelegung - im Ausland und/oder vor anderssprachigen Computern - sitzt).

Schreibt euch eure Passwörter auf!

Ja! Wie schon gesagt, jeder Login hat sein eigenes Passwort verdient & die Passwörter sollen lang und komplex sein. Da wir nun aber wissen, dass Passwörter so komplex sein sollen, dass ihr sie euch sowieso nicht merken könnt, speichert sie euch lieber verschlüsselt ab. Es gibt Passwortsafes, das ist Software, die eure Passwörter verwaltet und sie auf der Festplatte verschlüsselt abspeichert. Dieser 'Safe' wird mit einem besonders sicheren Passwort (dem Masterpasswort) gesichert. Dann ist es auch einfacher, für jeden Login ein eigenes Passwort zu haben. Das Passwort dafür muss natürlich stark sein! Am besten verwendet ihr als Masterpasswort eine Passphrase- das ist ein ganzer Satz, zum Beispiel: "Ich habe keine Ahnung von Security, oida, und das ist gut so!". Es sollte jedoch kein Zitat sein.
Eine Liste von Passwort-Management Software findet ihr unter dem Link zum Koubmit-Wiki am Ende dieses Flyers.
Noch kurz zu den Passwortsafes, die in aktuelle Browser eingebaut sind: Browser sind auf Desktoprechnern mittlerweile das Einfallstor Nummer 1 für Schadsoftware, also rechnet euch aus, wie sinnvoll es ist, denen das Verwalten von Passwörtern zu überlassen.
Noch 2 Tips zu Passwortsafes: Wer kein Backup hat, hat verkackt. Und zwar richtig, richtig ordentlich. Wer seine Passwörter, insbesondere das Masterpasswort, auf Computern eingibt denen sie/er nicht 100%ig vertraut, hat in der Regel ebenfalls verkackt.

Passwörter sollen regelmässig verändert oder ausgetauscht werden

In regelmässigen Zeitabständen solltet ihr euer Kreativitätszentrum im Hirn wieder aktivieren & euch ein neues Passwort ausdenken. Falls das ganze schnell gehen muss, weil es gerade stressig ist, ist es ein guter Tipp einfach mal ein paar Zeichen auszutauschen. Dies empfiehlt sich auch in Gruppen, weil dann bei Aenderungen nur noch gesagt werden muss: "Wir haben das Zeichen an Stelle X durch das Zeichen Y ersetzt". Dennoch soll das Passwort auch immer wieder ganz ausgetauscht werden!
Nehmt euch einen Kalender und zeichnet euch alle paar Monate einen Tag ein, den ihr zum Passwort ändern verwendet. Bei Gruppen ist es sinnvoll, das bei den grösseren Treffen zu machen, wo alle GenossInnen anwesend sind, die das Passwort wissen sollen.

Passwörter im Netz:

Verwendet immer verschlüsselte Verbindungen, wenn ihr Passwörter im Netz eingebt. Also https statt http, imaps statt imap, pop3s statt pop3 oder Verschlüsselung über TLS (Transport Layer Security). Es ist sonst möglich, die Daten die ihr über das Netz schickt mitzulesen und einfach das Passwort daraus zu extrahieren. Da hilft dann auch kein 48 Zeichen Passwort. Vertraut nicht darauf, dass die Verbindung 'eh sicher' ist. Vor allem bei unverschlüsselten WirelessLan Zugängen ist das wichtig.

Online Version des Password Strength Checkers (testet die Stärke von Passwörtern; Nur zum Testen! Keine echten Passwörter eingeben!):
https://www.hammerofgod.com/passwordcheck.aspx
Liste von Passwort-Managern im Koumbit-Wiki:
https://wiki.koumbit.net/PasswordManagementService/SoftwareOptions

tear the system down - bit. by. bit. mailto:bitbybit@riseup.net
technologie in linksradikalen kontexten irc://irc.indymedia.org/#bitbybit