Plattform 51a – LiveHack

Im Plattform 51a – LiveHack erwarten euch coole Projekte, geniale DIY´s und hilfreiche Tipps und Tricks. Heute geben wir euch ein paar Tipps, wie ihr euch und eure Daten besser im Internet schützen könnt.

Einzigartige und sichere Passwörter

Es ist zwar einfach und bequem, das gleiche Passwort überall zu benutzen, aber es bringt auch sehr viele Nachteile mit sich. Bei sehr wichtigen Konten sollte man verschiedene und Einzigartige Passwörter nutzen.
Ungeeignete Passwörter sind zum Beispiel: MamaIstDieBeste123 oder der Name des Haustieres usw.
Lieber sollte man ein Passwort mit Zahlen, Großbuchstaben und Sonderzeichen nehmen. So macht man zum Beispiel aus MaxMustermann das Passwort M4xMust3rm4nn2002!.
Somit ist man sicherer vor Hackern die einem Persönliche Daten stehlen wollen.

Von Diensten abmelden

Egal was ihr gerade im Internet gemacht habt, meldet euch immer von der Seite ab, wenn ihr fertig seid. Durch das Abmelden verringert Ihr die Wahrscheinlichkeit von Cross-Site-Request-Forgery-Angriffen. Das bedeutet, ein Hacker sagt eurem Browser, er soll Anfragen an andere Seiten schicken, bei denen ihr angemeldet seid. So kann er beispielsweise eine Banküberweisung anfragen. Passwörter sollten nicht auf dem Rechner gespeichert werden. So sind die eigenen Daten und Passwörter sicher.

Software aktuell halten

Software-Updates sind wichtig, da sie oft kritische Patches (Fehlerbehebungen) für Sicherheitslücken enthalten. Tatsächlich nutzen viele der gefährlichsten Malware-Angriffe, Software-Schwachstellen in gängigen Anwendungen wie Betriebssystemen und Browsern aus. Diese Patches verschließen die Sicherheitslücken und sichern eure Daten.

Sicherheiskopie gegen Ransomware

Wie würdet ihr reagieren, wenn ihr eines Tages den Zugriff zu wichtigen Dokumenten, Bildern und Videos verlieren würdet? Ransomware macht dieses Szenario zur Realität. Ransomware ist eine Art Malware, die Dateien auf deinem Gerät verschlüsselt. Für die Entschlüsselung deiner Dateien wird dann ein Lösegeld gefordert. Um online sicher zu sein, solltet Ihr Sicherheitskopien erstellen für den Fall, dass Euer Gerät verloren geht, gestohlen oder infiziert wird.

Auf der Hut vor Phishing-Angriffen

Phishing wird verwendet, an eure Anmeldedaten zu gelangen. Dabei wird ein bösartigen Link oder Anhang verschickt. Wenn ihr diesen öffnet, werdet ihr zu einer gefälschten Website weitergeleitet. Phishing wird neuerdings auch bei SMS und Chats eingesetzt. Öffnet also nicht direkt jede Mail oder SMS, wenn ihr nicht wisst, von wem sie kommt.

Der richtige Browser

Natürlich gibt es zahlreiche Browser, die sicher für die persönlichen Daten sind. Der mit Abstand sicherste Browser ist aber Firefox. Es gibt selbstverständlich Browser, die fast genau so gut sind und Extras wie eine VPN mitliefern. Aber im Großen und Ganzen sollte man zu Firefox tendieren.

Andere empfehlenswerte Browser wären Chrome, Opera GX, Safari und Tor.
Alle sind sicher und man ist anonym im Internet unterwegs.

Wir hoffen, dass diese Punkte euch weitergeholfen haben und das ihr jetzt mehr auf Euch im Internet aufpasst!