CyberPolice
Checkliste für Gewerbetreibende

Das A und O der IT-Sicherheit für Ihr Unternehmen – Tipps, die einfach in die Tagesroutine mit eingebaut werden können.	
Installieren Sie regelmäßig von den jeweiligen Herstellern bereitgestellte **Sicherheitsupdates** für Ihr Betriebssystem und die von Ihnen installierten Programme.	☐
Setzen Sie ein **Virenschutzprogramm** ein und aktualisieren Sie dieses regelmäßig, idealerweise über die Funktion „Automatische Updates“.	☐
Verwenden Sie eine **Personal Firewall**. Diese ist in den meisten modernen Betriebssystemen bereits integriert und soll Ihren Rechner vor Angriffen von außen schützen. Dazu kontrolliert sie alle Verbindungen des Rechners in andere Netzwerke und überprüft sowohl die Anfragen ins Internet als auch die Daten, die aus dem Internet an Ihren Rechner gesendet werden.	☐
Nutzen Sie für den **Zugriff auf das Internet** ausschließlich ein **Benutzerkonto mit eingeschränkten Rechten**, keinesfalls ein Administrator-Konto. Alle gängigen Betriebssysteme bieten die Möglichkeit, sich als Nutzer mit eingeschränkten Rechten anzumelden.	☐
Unterschätzen Sie Ihre Mitarbeiter als Gefahrenquelle nicht. Ihre Mitarbeiter sind die wichtigsten Firewalls Ihres Unternehmens. Sensibilisieren Sie diese für das Thema Sicherheit und **schulen Sie Ihre Mitarbeiter regelmäßig.**	☐
Nutzen Sie möglichst **sichere Passwörter.** Ändern Sie diese regelmäßig.	☐
Erstellen Sie einen Notfallplan.	☐
Achten Sie besonders auf **Datenschutz und –sicherheit.** Seien Sie besonders sorgfältig im Umgang mit sensiblen Daten und Geschäftsgeheimnissen.	☐
Seien Sie **zurückhaltend mit der Weitergabe persönlicher Informationen.** Seien Sie misstrauisch. Klicken Sie nicht automatisch auf jeden Link oder jeden Dateianhang, der Ihnen per E-Mail gesendet wird. Überprüfen Sie gegebenenfalls telefonisch, ob der Absender der Mail authentisch ist.	☐
Erstellen Sie **regelmäßig Sicherheitskopien „Backups“** Ihrer Daten, um vor Verlust geschützt zu sein. Hierzu können Sie beispielsweise eine Cloud-Speicher oder externe Festplatte nutzen. Bewahren Sie diese an einem anderen Ort auf, so dass diese von einem Schadenfall der Originale voraussichtlich nicht gleichzeitig betroffen sein können.	☐
Wenn Sie ein WLAN („Wireless LAN“, drahtloses Netzwerk) nutzen, dann sollte dies stets mittels des **Verschlüsselungsstandards WPA2** verschlüsselt sein.	☐
Überprüfen Sie in regelmäßigen Abständen den **Sicherheitsstatus Ihres Computers.**	☐

SIGNAL IDUNA
gut zu wissen

5708401 Feb18