Allgemeine Sicherheitstipps im Internet und im Online- und Mobile-Banking

Allgemeine Sicherheitstipps im Internet

- Nutzen Sie eine **(gekaufte & bekannte) Antivirensoftware** und richten Sie sich unbedingt eine **Firewall** ein.
- Nutzen Sie **sichere Passwörter**, die nicht leicht zu erraten sind!
- Ändern Sie Ihre Passwörter **regelmäßig** und nutzen Sie für Ihre verschiedenen Zugänge immer unterschiedliche Passwörter.
- Benutzen Sie für das Online-Banking **keine fremden Rechner** (z.B. im Internetcafé)! Denn Browser speichern Daten der letzten Verbindungen.
  Diese könnten später ausgelesen werden.
- Dies gilt auch für **öffentliche WLAN-Hotspots!** Konfigurieren Sie Ihr Handy so, dass es sich **nicht automatisch** in kostenlose WLAN-Netze **einwählt**.
- Windows User: Benutzer anlegen und **nicht als Administrator** arbeiten
- Verwenden Sie immer das **aktuelle Betriebssystem** mit allen verfügbaren Sicherheitsupdates!
- Nutzen Sie eine **sichere Verbindung** zum Internet und verschlüsseln Sie Ihre WLAN-Verbindung.
- Schalten Sie den Gastzugang aus und aktivieren Sie den Passwortschutz Ihres Routers.
- Wo möglich: Nutzen Sie eine **2 Faktor Authentifizierung** (2FA)
- Achten Sie darauf, dass die Daten **verschlüsselt übertragen** werden!
  Das erkennen Sie daran, dass die Seite mit „http**s**“ beginnt.
- Dies gilt sowohl für Partnerseiten als auch für den vertraulichen E-Mail-Verkehr.
- Wenn Sie auf Mobilität verzichten können, dann nutzen Sie einen **Zahlungsverkehrs-Software.**
- Falls Sie trotz aller Sicherheitsvorkehrungen verdächtige Kartentransaktionen bemerken oder Ihre Karten verlieren, dann steht Ihnen der **Sperr-Notruf** für alle Karten **und Ihren Online-Banking-Zugang** zur Verfügung.
- Unter **+49 116 116** erhalten Sie rund um die Uhr (24/7) Hilfe.
- Alternativ können Sie auch die Hotline der Kreditkartengesellschaft anrufen, die auf der Rückseite der Karte zu finden ist.

Kreissparkasse Saarpfalz

Online- und Mobile-Banking

- Keine Eingabe von persönlichen Daten (IBAN, PIN, Kartennummern, etc.) außerhalb des geschützten Online-Bankings.
- Keine Daten im Browser speichern, z.B. PIN und Anmeldenamen (Anmeldename kann von Ihnen geändert werden und PIN bis zu 38 Stellen möglich).
- Keine Links in E-Mails oder unbekannte Anhänge öffnen. (Den Link und den Absender immer genau lesen!)
- Adresse zum Banking immer per Hand eingeben (als Favorit auch OK).
- Kontoauszüge zeitnah kontrollieren (Kontowecker und Sparkassen-App helfen)
- Abmelden nach dem Banking, damit die Verbindung getrennt wird.
- Falls Ihnen etwas verdächtig vorkommt, dann informieren Sie sich bei Ihrer Sparkasse **bevor** Sie eine **TAN eingeben** und lassen Sie Ihr Online-Banking sperren.
- Alternativ können Sie Ihren Online-Banking-Zugang auch selbst sperren, indem Sie Ihre **PIN dreimal falsch** eingeben oder über das Formular im Service-Center der Internetfiliale (oder telefonisch über die 116 116)
- Die Sparkasse und ihre Verbundpartner **fragen niemals Ihre Passwörter / PIN's ab** (und drohen auf keinen Fall damit den Zugang zu sperren oder sonstiges).
- Bleiben Sie aufmerksam und legen Sie die max. Höhe Ihrer täglichen Verfügungen fest.

Hilfreiche Links

https://www.ksk-saarpfalz.de/sicherheit
https://www.ksk-saarpfalz.de/sicherheit-im-internet
https://identitaetsdiebstahl.info/
https://www.ksk-saarpfalz.de/de/home/login-online-banking/demo-online-banking-pushtan.html
https://www.bsi.bund.de

Kreissparkasse Saarpfalz