Infoblatt

Sicherheitshinweise KfW-Online-Banking

Hinweise zur sicheren Nutzung des Online-Kreditportals (OKP)

Bei der Nutzung des Online-Kreditportals bitten wir Sie, die nachfolgenden Sicherheitshinweise zu beachten. Sie minimieren damit Ihre Risiken und tragen so zu Ihrem eigenen Schutz bei.

Wie können Sie das KfW-Online-Banking sicher einrichten und verwalten?

- Das Online-Banking der KfW erreichen Sie über https://kfw.de/online-banking oder auch direkt mit https://onlinekreditportal.kfw.de.
- Nutzen Sie für das Online-Banking immer zwei Geräte. Das für den Empfang einer Transaktionsnummer (TAN) genutzte mobile Endgerät sollte nicht gleichzeitig für das Online-Banking genutzt werden.
- Unter der Rubrik "Meine Zugangsdaten" im Online-Kreditportal verwalten Sie die zur Anmeldung benötigte persönliche Identifikationsnummer (PIN) und die Verfahren für die Freigabe eines Auftrages (TAN-Verfahren).
- Hinterlegen Sie Ihre E-Mail-Adresse in den Kontaktdaten. Zusätzlich können Sie sich bei neuen und wichtigen Mitteilungen im elektronischen Postkorb per E-Mail informieren lassen.
- Prüfen Sie regelmäßig, mindestens einmal im Quartal, Ihren elektronischen Postkorb. Alle wichtigen Informationen stellen wir dort ein. Prüfen Sie auch regelmäßig Ihren Kontoauszug und die Kontobewegungen.

Was sollten Sie bei beim Umgang mit PIN und TAN beachten?

- Halten Sie grundsätzlich Authentisierungsinformationen (persönliche Identifikationsnummer und Transaktionsnummern) geheim und geben Sie diese nicht an Dritte weiter. Die KfW wird Sie niemals per Telefon oder E-Mail zur Herausgabe dieser Daten auffordern.
- Bei einer Neuregistrierung erhalten Sie Ihre persönliche Identifikationsnummer (PIN) per Post. Ändern Sie diese Initial-PIN nach der Aktivierung des TAN-Verfahrens und auch Ihre selbstvergebene PIN in regelmäßigen Abständen.
- Sofern Sie Ihre E-Mail-Adresse hinterlegt haben, können Sie sich bei Bedarf eine neue PIN über einen individuellen Aktivierungslink per E-Mail zusenden lassen.
- Eine PIN muss mindestens 12-stellig und darf maximal 30-stellig sein.
- Kombinieren Sie bei der Vergabe einer PIN Groß- und Kleinbuchstaben. Benutzen Sie auch Sonderzeichen. Erlaubt sind: *+,-./:;=?@_`§!#$%'()
- Die persönliche Identifikationsnummer darf nicht aus nur einem Zeichen (zum Beispiel: 111111111111) bestehen.
- Verzichten Sie auf gängige und leicht zu erratende Muster (zum Beispiel: 4711 oder Ihr Geburtsdatum).
- Eine neue persönliche Identifikationsnummer darf nicht identisch mit einer der letzten 5 verwendeten PINs sein.
- Verwenden Sie keine Passwörter mehrfach, zum Beispiel bei verschiedenen Portalen. Nutzen Sie jeweils ein individuelles Passwort.
- Bei diversen Funktionen des OKPs benötigen Sie zur Auftragsfreigabe eine einzelne Transaktionsnummer (TAN). Für die Anmeldung in das OKP ist keine TAN notwendig, nur die Eingabe der Geschäftspartnernummer und Ihrer PIN. Eine Aufforderung zur mehrmaligen Eingabe einer TAN auf einer vermeintlichen KfW-Seite sollte Sie misstrauisch machen.

Stand: 07/2024 • Bestellnummer: 600 000 1550
KfW Bankengruppe • Palmengartenstraße 5-9 • 60325 Frankfurt
Infocenter • Telefon: 0800 539 9003 (kostenfrei) • Fax: +49 69 7431 9500 • www.kfw.de

Infoblatt

Sicherheitshinweise KfW-Online-Banking

Was können Sie selbst zur Sicherheit Ihrer Hard- und Software beitragen?

- Prüfen Sie eingehende E-Mails immer aufmerksam, auch bei scheinbar bekannten Absenderadressen. Diese könnten Schadsoftware und gefälschte Links enthalten oder dazu dienen, unter einem Vorwand vertrauliche Informationen von Ihnen zu erhalten.
- Seien Sie achtsam bei eingehenden unbekannten Anrufen. Geben Sie telefonisch keine vertraulichen Informationen zu Ihrem Online-Banking weiter.
- Legen Sie für Ihr Betriebssystem unterschiedliche Benutzerkonten an. Verwenden Sie im digitalen Alltag nur Benutzerkonten mit eingeschränkten Rechten. Dies kann verhindern, dass Schadsoftware über Administratorrechte installiert wird.
- Verwenden Sie immer aktuelle Versionen des Betriebssystems und Webbrowsers. Deaktivieren Sie nicht von Ihnen benötigte Erweiterungen.
- Führen Sie regelmäßig Software-Updates durch und nutzen Sie hierfür auch Funktionen zur automatischen Aktualisierung.
- Aktivieren Sie ein integriertes Virenschutzprogramm sowie eine Firewall oder verwenden Sie alternative Programme.
- Deinstallieren Sie ungenutzte Programme und Anwendungen.
- Wählen Sie für die Datenschutzeinstellungen des Webbrowsers ein möglichst hohes Niveau.
- Speichern Sie häufig aufgesuchte Internetseiten als Lesezeichen oder Favorit und achten Sie auf das Kürzel "https://" für sichere Internetadressen.
- Öffentliche WLAN-Hotspots sind häufig nicht ausreichend abgesichert. Verzichten Sie hier auf Online-Banking und das Übermitteln vertraulicher Daten. Nutzen Sie möglichst Ihre eigenen Geräte, um auf Ihr Online-Banking zuzugreifen – auch wenn Sie im Urlaub oder anderweitig unterwegs sind.
- Beenden Sie eine Online-Sitzung immer durch korrektes Abmelden, nicht durch einfaches Schließen des Browserfensters. Löschen Sie dabei auch im Browser gespeicherte Informationen wie den Verlauf, Formulardaten und Kennwörter. Vor allen Dingen, wenn Sie öffentliche Geräte oder Geräte anderer Personen nutzen.
- Lassen Sie Ihre Geräte niemals unbeobachtet und nutzen Sie auch Funktionen für eine automatische Bildschirmsperre.
- Schauen Sie bei der Eingabe von PINs und Passwörtern immer darauf, dass Sie von niemandem beobachtet werden können.
- Nutzen Sie nur vertrauenswürdige Quellen für den Download von Daten und Programmen. Informieren Sie sich gegebenenfalls vorab über die Seriosität der Datenquelle und den Herausgeber.
- Schützen Sie persönlichen Daten und wichtige Dateien durch Verschlüsselung.
- Erstellen Sie regelmäßig Sicherheitskopien auf einem externen Datenträger.
- Löschen Sie alle persönlichen Informationen und Dateien bei einem Verkauf oder der Gerätentsorgung.

Stand: 07/2024 • Bestellnummer: 600 000 1550
KfW Bankengruppe • Palmengartenstraße 5-9 • 60325 Frankfurt
Infocenter • Telefon: 0800 539 9003 (kostenfrei) • Fax: +49 69 7431 9500 • www.kfw.de

Infoblatt

Sicherheitshinweise KfW-Online-Banking

Was können Sie im Notfall tun?

- Wechseln Sie bei Verdacht einer missbräuchlichen Verwendung Ihrer Nutzerdaten unverzüglich die persönliche Identifikationsnummer (PIN).
- Sperren Sie gegebenenfalls Ihren Online-Zugang. Am schnellsten geht das, indem Sie selbst dreimal eine falsche PIN eingeben. Ihr Zugang ist dann sofort gesperrt. Gerne können wir Ihren Zugang auch telefonisch sperren. Sie erreichen uns kostenfrei unter: 0800 539 9003. Wir helfen Ihnen gerne.
- Sichern Sie Beweise wie E-Mails oder Screenshots der Internetseiten. Erstatten Sie im Schadensfall Anzeige bei der Polizei.
- Kontaktieren Sie uns, wenn Sie den Verdacht einer missbräuchlichen Verwendung Ihrer Daten haben oder Sie unsicher sind, ob eine E-Mail oder Internetseite der KfW authentisch ist.

Stand: 07/2024 • Bestellnummer: 600 000 1550
KfW Bankengruppe • Palmengartenstraße 5-9 • 60325 Frankfurt
Infocenter • Telefon: 0800 539 9003 (kostenfrei) • Fax: +49 69 7431 9500 • www.kfw.de