Bergedorf Bille
Gemeinnützige Baugenossenschaft eG

Sicherheitshinweise für das Internet

Mit wenigen Handgriffen können Sie zur Sicherheit Ihres PC beitragen:

1. **Nutzen Sie ein aktuelles PC-Betriebssystem**

   Aktualisieren Sie Ihr PC-Betriebssystem regelmäßig. Hierdurch werden häufig bestehende Sicherheitslücken geschlossen. Wir empfehlen Ihnen, die kostenfreie automatische Updatefunktion des Betriebssystems zu nutzen. Alternativ können Sie sich die Updates von der Internet-Seite des Herstellers herunterladen. Die Updates stehen Ihnen kostenfrei zur Verfügung.

2. **Schützen Sie Ihren Computer mit aktueller Sicherheitssoftware**

   Setzen Sie einen aktuellen Virenscanner ein. Virenscanner schützen Ihren Computer, indem Viren, trojanische Pferde und Würmer in empfangenen und vorhandenen Daten gefunden und vernichtet werden. Aktualisieren Sie vor jedem Besuch im Internet Ihren Virenscanner. Nutzen Sie auch hier die automatischen Updatefunktionen.

   Lassen Sie regelmäßig Ihren gesamten Datenbestand auf Ihrem Computer durch den Virenscanner überprüfen.

   Setzen Sie eine aktuelle Personal-Firewall ein. Personal-Firewalls schützen Sie vor unerwünschten Zugriffen von außen und trennen auf Wunsch unerlaubte Verbindungen. Aktualisieren Sie regelmäßig Ihre Personal-Firewall. Nutzen Sie die automatischen Updatefunktionen.

   Aktuelle Sicherheitssoftware erhalten Sie im Fachhandel oder kostenlos im Internet.

3. **Aktivieren Sie die richtigen Internet-Browser-Einstellungen**

   Bei der Auswahl eines Internet-Browsers sollten Sie beachten, dass er von vertrauenswürdigen Quellen stammt.

   Über die Internet-Seite des Herstellers können Sie kostenlos Ihren Browser durch Updates aktualisieren. So schließen Sie neu erkannte Sicherheitslücken. Um z.B. den Internet-Explorer von Microsoft zu aktualisieren, wählen Sie im Menü „Extras“ und anschließend „Windows-Update“. Folgen Sie der Menüführung, um die aktuelle Version zu installieren.

   Stellen Sie Ihren Browser so ein, dass Sie immer über alle sicherheitsrelevanten Vorgänge informiert werden. Zum Beispiel gibt der Internet-Explorer Hinweise, wenn Sie in einem gesicherten Bereich (https://...) wechseln bzw. einen gesicherten Bereich verlassen (http://...).

   In vielen Browsern gibt es eine Funktion, Benutzernamen und Passwörter bei Zugängen zu Internetseiten zu speichern. Die Funktion heißt „Auto vervollständigen“ oder „Form-Manager“. Aus Sicherheitsgründen sollte diese nicht benutzt werden, da sonst sensible Daten auf Ihrem Computer gespeichert werden. Dritte können diese auslesen und Ihrer EDV Schaden zufügen.

   Wir empfehlen, die Verlaufs- bzw. History-Einträge nach Beendigung Ihrer Internet-Aktivitäten zu löschen. Hinweise zur Löschung erhalten Sie über das Hilfe-Menü Ihres Internet-Browsers.

   Ein sicherheitsbewusstes Verhalten im Internet schützt Sie und Ihren Computer vor unberechtigten Zugriffen

Stand: Januar 2018

4. **Nutzen Sie nur Programme mit bekannter Herkunft**

Installieren Sie auf Ihrem Computer nur Programme, die Sie aus vertrauenswürdigen Quellen bezogen haben. Mit Programmen können Viren oder trojanische Pferde übertragen werden. Verzichten Sie bei zweifelhaften oder unbekannten Quellen auf eine Installation. Erhalten Sie Programm über einen Datenträger (z.B. Disketten, CD etc.), prüfen Sie diese vorher mit einem aktuellen Virenscanner.

5. **Verhalten Sie sich richtig im Umgang mit E-Mails**

Die Übertragung von Viren oder trojanischen Pferden kann auch per Dateianhang in E-Mails geschehen. Öffnen Sie deshalb keine Dateianhänge aus E-Mails, deren Absender nicht kennen. Seien Sie ebenfalls bei E-Mails aus Ihrem Bekanntenkreis vorsichtig. Sofern ein Computer mit Viren infiziert ist, erfolgt die Verbreitung der Viren oft automatisch in alle Einträge Ihres Adressbuches.

Entdecken Sie Unregelmäßigkeiten, löschen Sie die E-Mail sofort!

Die Baugenossenschaft wird Sie niemals per E-Mail, telefonisch oder persönlich auffordern, sensible Kundendaten zur Überprüfung anzugeben. Sie werden ebenso niemals E-Mails erhalten, die Sie auffordern eine Internetseite zu öffnen und dort Kundendaten wie Kontonummer oder PIN einzugeben. Verlassen Sie sich nicht auf das Aussehen der Seite, sondern überprüfen Sie deren Echtheit.

Nehmen Sie sofort Kontakt mit uns auf, wenn Sie auf eine betrügerische E-Mail geantwortet oder auf einer Seite Ihre Daten eingegeben haben.

6. **Beschreibung des PIN-Verfahrens**

Damit niemand unberechtigt auf Ihre Konten zugreifen kann, wird das PIN-Verfahren (PIN = Persönliche Identifikationsnummer) eingesetzt. Bei Ihrer ersten Anmeldung zum Home-Banking der Baugenossenschaft werden Sie nach Eingabe der Start-PIN automatisch aufgefordert, die Start-PIN in eine eigene 5-stellige PIN, die aus Ziffern, Buchstaben und bestimmten Sonderzeichen bestehen kann, zu wechseln. Mit dieser Änderung der Start-PIN steht Ihnen unsere Home-Banking-Anwendung mit Ihrer persönlichen PIN zur Verfügung. Beim Anmelden zum Home-Banking geben Sie Ihre Kontonummer und PIN ein. Sie können sich nun den Kontostand und die Umsätze anzeigen lassen.