



Gebote für Ihre Internet-Sicherheit

**Onlinebanking ist die Zukunft sämtlicher Bankgeschäfte.
Doch leider sind damit auch Risiken und Gefahren verbunden.**

Wir möchten Sie mit diesen Informationen nicht bevormunden, sondern Sie aktiv im Sinne Ihrer Sicherheit aufklären und sensibilisieren.

1 Verwenden Sie eine Firewall!

Verbinden Sie niemals Ihren Computer ohne Firewall oder DSL-Router mit dem Internet und überprüfen Sie regelmäßig Ihre(n) Firewall / DSL-Router auf Fehlkonfigurationen und evtl. Sicherheitslücken.

2 Arbeiten Sie auf Ihrem PC als „Benutzer“ ohne administrative Berechtigungen!

Eine Hauptursache für Infektionen vom Computern durch Viren, Würmer und Trojanische Pferde ist das Surfen und Mailen mit Hauptbenutzer- oder Admin-Rechten!

Verwenden Sie deshalb beim Surfen und Mailen im Internet immer einen Benutzer mit eingeschränkten Benutzerrechten. Surfen Sie niemals mit Hauptbenutzer- oder Adminberechtigungen.

3 Setzen Sie nur aktuelle Software ein!

Nutzen Sie für Ihren PC, mit dem Sie im Internet surfen oder Mails versenden, ausschließlich **aktuelle Betriebssystemsoftware (Windows VISTA ,Windows 7 und Windows 8 mit aktuellem Service Pack) und aktuelle Anwendungssoftware**. Alte Systeme entsprechen nicht mehr den aktuellen SicherheitSanforderungen.

Installieren Sie unbedingt alle angebotenen Systemupdates für Ihr Betriebssystem, verwenden Sie optimaler weise die Einstellung „ Updates automatisch herunterladen und installieren“.

Aktualisieren Sie auch regelmäßig Ihren Webbrowser, E-Mail Client, Firewall, DSL-Router, Anti Virus Software.

4 Verwenden Sie eine professionelle Anti Virus Software!

Installieren Sie unbedingt eine professionelle Anti Virus Software auf Ihrem Computer. Vergleichen Sie dazu regelmäßig Testberichte in gängigen Computer-Fachzeitschriften.

5 Öffnen Sie nicht jeden E-Mail Anhang!

Viren, Würmer und Trojanische Pferde werden gern über E-Mail Anlagen auf den PC eingeschleust. Bedenken Sie, dass auch Fotos, Videofilme, PDF-Dokumente, Office-Dokumente usw. Viren enthalten können.

„Ein Gedanke vor dem Klick, das ist hier der Sicherheits-Trick“!



6 Verwenden Sie das „Textformat“ für E-Mails!

Sollten Sie einen E-Mail Clienten wie Outlook oder Windows Mail verwenden, dann nutzen Sie zu Ihrer Sicherheit das Darstellungsformat „Textformat“ und nicht das HTML-Format. Im HTML-Format können für Sie unsichtbare „Schädlinge“ versteckt werden, die sich schon allein beim Anzeigen des E-Mails aktivieren.

Klicken Sie möglichst nicht auf weiterleitende Links in E-Mails, wenn Sie sich dessen nicht sicher sind!!

7 Geben Sie niemals vertrauliche Daten weiter!

Schützen Sie Ihre vertraulichen Daten wie Kennwörter, PINs, TANs, Passwörter usw. und geben Sie diese niemals an dritte Personen weiter!!

8 Surfen Sie nicht auf jeder Internetseite!

Meiden Sie möglichst unseriöse Internetseiten und Seiten, auf denen Dritte Dateien (wie z. Bsp. Videos, Filme usw.) hochladen können.

9 Installieren Sie niemals Software fragwürdiger Herkunft!

Verwenden Sie möglichst nur Software aus vertrauenswürdigen Quellen, da so genannte „gecrackte Software“ Trojanische Pferde enthalten können, die dann von Ihnen auch nicht erkannt werden.

10 Schützen Sie Ihr WLAN!

Kriminelle Täter suchen nach nicht ausreichend geschützten WLANs und verbinden sich über diese mit dem Internet, um Straftaten zu begehen. Verwenden Sie deshalb den Verschlüsselungsstandard „WPA2“ mit einem 63 Zeichen langen Kennwort!

Ihre
Bopfinger Bank
Sechta-Ries eG