SPARKASSE
CASSA DI RISPARMIO

WIE SIE SICH VOR CRIMEWARE SCHÜTZEN KÖNNEN

Einige Vorkehrungen können sich als nützlich erweisen, um der Verbreitung dieses Betrugsphänomens entgegenzuwirken. Besonders hilfreich sind dabei folgende Maßnahmen:

1. Schützen Sie Ihren für das Internet Banking verwendeten PC durch die **Installation einer Anti-Virus-Software** gegen Computerseuchen. Einige Unternehmen bieten auch eine spezifische Anti-Spyware-Software an, die Sie zusätzlich auf Ihrem PC installieren können.
2. Führen Sie **regelmäßige Scans** und laufende **Updates Ihrer Anti-Virus-Software** (und der evtl. installierten Anti-Spyware-Software) durch und überprüfen Sie die ständige **Verfügbarkeit der Verbindung** zur Website des Softwareherstellers.
3. **Aktualisieren Sie laufend den Schutz** des Betriebssystems und der Anwendungs-software ihres PCs durch die Installation von so genannten **Patches** (wörtlich “Flicken”, weil sie die Schwachstellen abdecken), die von den jeweiligen Herstellern zur Verfügung gestellt werden. Installieren sie nur **offizielle Updates**, die auf den Internetseiten der Hersteller kostenlos bereitgestellt werden.
4. **Schützen Sie den ein- und ausgehenden Datenverkehr** auf ihrem PC durch die Installation geeigneter Kommunikationsfilter, so genannter **Firewalls**.
5. Achten Sie beim Surfen im Internet darauf, dass keine **unbefugten Aktivitäten** von außen durchgeführt werden und installieren Sie nur Programme aus dem Web, deren Herkunft überprüfbar ist.
6. Wenn der **PC infiziert** ist, kommt es häufig zu ungewollten Änderungen der Systemeinstellungen und zu einer Verschlechterung der Computerleistung (z.B. langsame Ausführung von Befehlen, ungewollte Öffnung von Pop-Up-Fenstern). Beobachten Sie derartige Änderungen aufmerksam, denn sie sind Anzeichen einer möglichen Infizierung.
7. Seien Sie misstrauisch, wenn Sie Nachrichten (per E-Mail, über Webseiten, Instant-Messaging-, Chat-, oder Peer-to-Peer-Kontakte) erhalten, in denen Sie aufgefordert werden, **Programme oder Dokumente unbekannter Herkunft herunterzuladen**.
8. Seien Sie vorsichtig, wenn Sie **Anomalien** feststellen oder in einer von den üblichen Modalitäten abweichenden Form zur Eingabe Ihrer persönlichen Daten auf **Ihrer Home-Banking-Seite** aufgefordert werden.
9. **Überprüfen Sie die Authentizität der Verbindung zu Ihrer Bank**, indem Sie den Namen der Internetseite genau kontrollieren. Falls vorhanden, können Sie die Richtigkeit der Angaben über das Zertifikat der Seite, zu der die Verbindung aufgebaut wird, auch durch einen Doppelklick auf das Symbol des Sicherheitsschlosses (oder des Schlüssels) im Browser-Fenster überprüfen.
10. **Kontrollieren Sie regelmäßig Ihre Kontoauszüge**, um sicherzustellen, dass die aufgeführten Vorgänge tatsächlich von Ihnen ausgeführt wurden. Ist das nicht der Fall, wenden Sie sich umgehend an Ihre Bank.