Sparkassen Versicherung

Tipps für mehr Sicherheit im Internet

Ein Leben ohne Internet ist in der heutigen Zeit kaum noch vorstellbar. Doch gerade in der virtuellen Welt verbergen sich viele Risiken. Wie Sie sich mit kleinen Tricks schützen können, verraten wir Ihnen gerne.

Passwörter

Passwörter sind oft der einzige Schutzmechanismus, den Sie für Ihre privaten Daten haben. Doch bei der richtigen Passwortfindung tun sich viele Nutzer schwer. Oft kommt es deshalb vor, dass man ein Passwort für alle Programme oder Zugänge hat. Das freut Hacker ganz besonders. Sie haben Werkzeuge, die vollautomatisch so genannte „Wörterbuchangriffe“ durchführen. Sie können ganze Wörter aus dem Wörterbuch einschließlich gängiger Kombinationen aus angefügten Zahlen und Sonderzeichen testen. Um das zu verhindern, sollten Ihre Passwörter bestimmte Qualitätsanforderungen erfüllen. Inzwischen ist es üblich, dass man sich bei unterschiedlichsten Anbietern im Internet ein Konto oder einen Zugang (Account) anlegen kann. Die Anmeldung an diesem Account wird mit einem Passwort geschützt. Was könnte passieren, wenn sich jemand unter Ihrem Namen dort anmeldet? Wer möchte schon gerne, dass Fremde unter dem eigenen Namen E-Mails verschicken oder teure Waren im Internet ersteigern können?

Tipps zum Erstellen eines sicheren Passworts:

- das Passwort sollte mindestens 10 Zeichen haben
- Groß- und Kleinbuchstaben, Zahlen und Sonderzeichen
- keine Umlaute, denn diese sind im Ausland oft nicht möglich
- keine Wörter aus dem Wörterbuch
- „willkürlich gewählte“ Buchstaben mit Hilfe von Eselsbrücken merken: „Sonntag ist mein Lieblingstag, weil ich da bis 10 Uhr ausschlafen kann“ > Passwort: „SimL,widb10Uak“
- einfache Ziffern oder Sonderzeichen wie „?“ am Anfang oder Schluss eines sonst sehr einfachen Passworts helfen nicht

Weitere Tipps:

- Ändern Sie Ihre Passwörter mindestens alle 6 Monate
- Benutzen Sie unterschiedliche Passwörter
- Geben Sie keine Passwörter weiter

Online-Banking

Online-Banking bezeichnet die Abwicklung von Bankgeschäften über das Internet. Dabei sind neben Abfragen von Kontostand und Umsätzen auch die Durchführung von Überweisungen, die Einrichtung von Daueraufträgen oder Geldanlagen möglich. Kriminelle versuchen oft, Konto- und Kreditkartendaten der Nutzer auszuspähen, um so an das Geld der Bankkunden zu kommen.
Hier ist besondere Sicherheit geboten, da Ihr Geld im direkten Visier der Kriminellen steht.

Pharming:
Ist eine Betrugsmethode, bei der sich der Täter durch das Umleiten des Internetnutzers auf gefälschte Webseiten durch Manipulation des Webbrowsers vertrauliche Zugangs- und Identifikationsdaten von arglosen Dritten verschafft. Mit den gewonnenen Daten nimmt der Täter unter der Identität des Inhabers im Online-Verkehr unerlaubte Handlungen vor.

Tipps für eine sichere Online-Banking-Nutzung:

- Verschlüsseln Sie Ihre WLAN-Verbindung. Standard ist heute WPA 2 (Wi-Fi Protected Access 2), wobei das Passwort mindestens 20 Zeichen lang sein sollte. WEP (Wired Equivalent Privacy) ist hingegen veraltet und gilt darum als unsicher.
- Teilen Sie niemals Ihre Anmeldedaten mit anderen, speichern Sie die Anmeldedaten auch nicht in Ihrem Browser.
- Achten Sie beim Online-Banking darauf, dass die Kommunikation verschlüsselt erfolgt. Online-Banking sollte immer über das geschützte https-Protokoll erfolgen. Ob das der Fall ist, können Sie daran erkennen, dass sich der Anfang der Browserzeile verändert. Statt http:// wird dann https:// angezeigt.
- Sollten Sie eine E-Mail von Ihrer Bank erhalten mit der Aufforderung zur Eingabe Ihrer Anmeldedaten oder von Transaktionsnummern, löschen Sie diese sofort. Das ist ein Betrugsversuch.

- Folgen Sie nie einem Link zur Anmeldung im Online-Banking. Öffnen Sie die Seite lieber immer direkt.
- Halten Sie Ihr Betriebssystem und Ihren Anti-Viren-Schutz immer aktuell, um Sicherheitslücken zu schließen.
- Prüfen Sie bei jeder Transaktion die angezeigten Daten vor der TAN-Eingabe und nach der Transaktion Ihre Umsätze. So können Sie die Gefahr erkennen und abwenden.
- Wenn Sie Online-Banking über Ihr Smartphone nutzen, achten Sie auf eine Bildschirmsperre für Ihr Gerät und nutzen Sie Passwörter für Banking-Apps. Ebenso sollten Sie eine gültige Anti-Virus-Software auf Ihrem Smartphone installieren.
- Legen Sie ein Überweisungslimit mit Ihrer Bank fest. So kann nur eine begrenzte Summe pro Transaktion überwiesen werden.
- Sollte Ihnen etwas verdächtig vorkommen, dann lassen Sie Ihren Zugang von der Bank sperren.

Online-Shopping

Die Einkaufsgewohnheiten der Menschen haben sich grundlegend geändert. Die meisten kaufen ihre Waren und Dienstleistungen vorrangig im Internet. Statt im Einkaufszentrum ewig nach einem Parkplatz suchen zu müssen und sich kurz vor Ladenschluss noch durch die überfüllten Gänge zu quetschen, ziehen viele das Online-Shopping bequem von zu Hause aus vor. Dabei lockt neben der großen Auswahl auch die Globalisierung. Zwischenzeitlich ist es kein Problem mehr, sich im Ausland Waren zu bestellen und bis in die eigene Wohnung liefern zu lassen.
Doch durch die Anonymität im Netz gibt es auch viele Betrüger. Diese erstellen Online-Shops, kassieren den Kaufpreis, aber auf die bestellten Waren können Sie umsonst warten. Doch nicht nur beim Einkauf von Waren kann es zu Betrügereien kommen, auch wenn Sie Ihre gebrauchten Gegenstände online verkaufen wollen, warten Risiken auf Sie.

Tipps wie Sie einen seriösen Online-Shop erkennen können:

- Ist der Auftritt seriös? Übersichtlicher und strukturierter Aufbau? Ohne Rechtschreibfehler?
- Ist ein Impressum und Ansprechpartner vorhanden?
  - Name, Vorname und vollständige Anschrift des Anbieters
  - Informationen zur schnellen Kontaktaufnahme (Telefonnummer, E-Mail, Fax)
  - Gewerberegister und Gewerberegisternummer
  - Unternehmensname und Rechtsformzusatz
  - Umsatzsteuer-Identifikationsnummer
  - Angabe der Aufsichtsbehörde (sofern das Angebot einer Zulassung bedarf z. B. Apotheker)
- Sie können eine Test-E-Email an den Online-Shop versenden und es kommt eine kompetente Antwort zurück?
- Lesen Sie Erfahrungsberichte und Bewertungen des Shops. Bei Online-Auktionen sind die Bewertungen der Verkäufer zu beachten.
- Beachten Sie die Datenschutzbestimmungen. Werden meine Daten an Dritte weitergegeben?
- Sind Informationen über den Widerruf vorhanden?
- Gibt es Gütesiegel, die einen sicheren Shop kennzeichnen?

- Spätestens beim Bezahlen sollten Sie auf eine sichere Seite verwiesen werden, achten Sie deshalb darauf, dass die Seite mit https:// beginnt. Eventuell erscheint sogar ein Schloss in der Adresszeile.
- Auch im Internet gilt: Niemand hat etwas zu verschenken, sind Angebote zu schön um wahr zu sein, sind sie dies wahrscheinlich auch nicht > orientieren Sie sich an der Konkurrenz.
- Bewahren Sie nach dem Online-Einkauf die Kaufdaten auf (Uhrzeit, Quittungsnummer, Auftragsbestätigung, …)
- Überprüfen Sie in regelmäßigen Abständen Ihre Kreditkartenabrechnungen. Sollten Sie Unregelmäßigkeiten erkennen, wenden Sie sich sofort an Ihre Bank.

Anti-Virus-Software/Anti-Spyware

Wer ärgert sich nicht, wenn er durch einen Virusinfekt krank zu Hause bleiben muss, um eine Erkältung richtig auszukurieren. Mindestens genauso ärgerlich ist eine Virusattacke auf dem Computer, Smartphone oder Tablet. Mit einfachen Maßnahmen können Sie Ihre Sicherheit im Internet erhöhen. Anti-Viren-Software dienen zur Abwehr von Viren und Trojanern.

Tipps für die Auswahl Ihres Anti-Viren-Schutzes:

- Installieren Sie eine Schutzsoftware auf allen Ihrer Geräte und nicht nur auf dem PC
- Beachten Sie, dass eine Bezahlsoftware mehr Schutz bietet, als Freeware
- Laden Sie die Programme grundsätzlich von den Herstellerwebseiten herunter. Nur so können Sie sicher sein, dass das Programm aktuell ist.
- Aktualisieren Sie die Software regelmäßig, nur so kann auch eine Abwehr der neusten Viren sichergestellt werden.
- Viele Virenschutzprogramme müssen jährlich verlängert werden. Behalten Sie diesen Termin im Blick, um den Schutz nicht zu verlieren.
- Achten Sie darauf, dass Ihr Betriebssystem und Ihre Programme immer auf dem neuesten Stand sind. So können keine Schwachstellen entstehen, die von Hackern oder von Schadsoftware ausgenutzt werden können.

Spam-E-Mails

Jeder hat sicherlich schon eine Spam-E-Mail erhalten. Diese Spam-E-Mails enthalten oftmals Kettenbriefe, Werbebeiträge in sozialen Netzwerken oder den Massenversand von nichtangeforderten Werbe-E-Mails. Über diese E-Mails werden häufig Trojaner, Schadsoftware, Viren oder ähnliches versendet. Zudem gibt es Phishing-E-Mails, die über gefälschte E-Mails an persönliche Daten eines Internet-Benutzers zu gelangen, um damit Identitätsdiebstahl zu begehen. Typisch ist die Nachahmung einer Bank-E-Mail.

Phishing:
Ist eine Betrugsmethode, bei der sich der Täter mit Hilfe gefälschter E-Mails vertrauliche Zugangs- und Identifikationsdaten von arglosen Dritten verschafft, wobei der Täter typischerweise ein durch die Täuschung über die tatsächliche Identität erlangtes Vertrauensverhältnis ausnutzt. Mit den gewonnenen Daten nimmt der Täter unter der Identität des Inhabers im Online-Verkehr unerlaubte Handlungen vor.

Tipps im Umgang mit solchen E-Mails:

- Seien Sie vorsichtig mit E-Mails, die in Ihrem Spam-Ordner landen. Öffnen Sie diese nur, wenn Sie sich sicher sind, dass diese von einem sicheren Absender stammen.
- Öffnen Sie keine Links von unbekannten oder unerwünschten Absendern
- Folgen Sie keinen Links von unbekannten oder unerwünschten Absendern
- Folgen Sie keinen Aufforderungen unseriöser E-Mails > unseriöse E-Mails erkennen Sie z.B. an Rechtschreibfehlern, Grammatikfehlern oder wenn Sie nicht mit Ihrem richtigen Namen angeschrieben werden (Peter2Müller@lala.de > Hallo Peter2 Müller)
- Phishing E-Mails sind oftmals schwer zu enttarnen, da Sie oft legitim aussehen und als Absender Unternehmen angeben, die sie normalerweise kennen. Bedenken Sie jedoch, dass Banken etc. Sie niemals Daten per E-Mail abfragen und Sie direkt auf diese E-Mail antworten müssen oder über einen Link > wenn Sie dennoch unsicher sind, gehen Sie direkt auf die Homepage des betroffenen Unternehmens und loggen sich auf der offiziellen Seite ein, und überprüfen ob Ihre Daten korrekt sind.

Soziale Netzwerke

Sharing, also Inhalte mit anderen Personen zu teilen, ist ein gemeinsames Merkmal von Social-Media-Plattformen. Doch Sie sollten sich gut überlegen, ob Sie Ihre persönlichen Inhalte allen Nutzern zur Verfügung stellen wollen oder manche Inhalte privat halten bzw. nur einer ausgewählten Gruppe von Freunden oder so genannten Follower zugänglich machen. Denken Sie immer daran, dass auch kommerzielle Institute Ihre Daten weiterverwenden können. Merken Sie sich immer eines: das Internet vergisst nichts!

Tipps zum Umgang mit sozialen Netzwerken:

- In so gut wie allen sozialen Netzwerken können Sie mit Hilfe der Datenschutz-Einstellungen kontrollieren, überprüfen und einschränken, wer Ihre Daten sehen soll.
- Jedoch kann nie genau sichergestellt werden, wer die Bilder und Dateien einsehen oder verwenden kann, deshalb gilt Vorsicht bei der Veröffentlichung!
- Überlegen Sie sich genau, welche Bilder Sie hochladen > posten Sie keine Bilder, die Sie selbst (oder eine andere Person) unter dem Einfluss von Alkohol oder anderen Substanzen zeigen.
- Wenn Sie Bilder von anderen Personen veröffentlichen oder Bilder, die eine andere Person aufgenommen hat, holen Sie sich die Erlaubnis ein, sonst kann ein Copyright-Verstoß vorliegen.
- Überlegen Sie sich gut, wie viele Daten Sie von sich preisgeben möchten (Telefonnummer, Adresse, …), denn dies kann negative Auswirkungen auf Ihre Privatsphäre oder auf Ihre Sicherheit haben.
- Bevor Sie Informationen über einen geplanten Urlaub posten, sollten Sie daran denken, dass dies die Aufmerksamkeit von Einbrechern auf sich ziehen kann.
- Beachten Sie auch, dass auf Online-Portalen viele Betrüger unterwegs sein können, glauben Sie nicht jedem, der Kontakt mit Ihnen aufnimmt.

Mobbing

Soziale Netzwerke haben Mobbing eine neue öffentliche Qualität verschafft. Personen können zum Beispiel bewusst aus Gruppen ausgeschlossen werden oder digitale Pinnwände mit Beleidigungen beschrieben werden. Dies kann zu einer Belastung werden, vor allem für Jugendliche. „Cyberstalker“ können sich unechte Profile anlegen, in denen sie sich als eine reale Person ausgeben. Die Anonymität des Internets lässt diese Personen ohne Probleme andere belästigen. Freundschaften sind in sozialen Netzwerken schneller geschlossen als in der „realen“ Welt. So können Informationen an Personen gelangen, die so nie anvertraut werden. Dieses Risiko haben vor allem Kinder und Jugendliche. Betrüger können dadurch an Verabredungen mit den Kindern kommen.

Tipps im Umgang mit Mobbing:

- Beleidigende oder sogar bedrohliche E-Mails dürfen nicht toleriert werden. Kinder und Jugendliche sollten aber nicht direkt auf solche E-Mails oder SMS antworten, sondern Eltern und andere Vertrauenspersonen einbeziehen.
- Vertrauen Sie sich Freunden oder Bekannten an. Bei Schülern sollte die Schule informiert werden.
- Bewahren Sie Beweismaterial auf: Speichern Sie die verbreiteten Bilder, E-Mails und SMS.
- Wenden Sie sich in schwerwiegenden Fällen direkt an die Polizei und erstatten Sie Anzeige.
- Bilder und Videos, die ohne Erlaubnis des darin Gezeigten veröffentlicht werden, sollten immer wieder gelöscht werden. Die Löschung kann über den Netzwerk-Betreiber vorgenommen werden. Auch so genannte „Fake-Profile“ können so auch aus dem Netzwerk entfernt werden.

Hilfreiche Seiten:

- Bundesamt für Sicherheit in der Informationstechnik: https://www.bsi-fuer-buerger.de/BSIFB/DE/Home/home_node.html
- Bundeskriminalamt: http://www.bka.de/DE/ThemenABisZ/Deliktsbereiche/InternetKriminalitaet/internet-Kriminalitaet__node.html?__nnn=true
- LKA Niedersachsen: http://www.polizei-praevention.de/home.html
- Kinderschutz im Internet: http://www.sicher-online-gehen.de/
- Klick-Safe: http://www.klicksafe.de/service/materialien/broschueren-ratgeber/surfen-kinder-sicher-online/

Lexikon Cyber-Risiken für Privatpersonen

Botnetze
sind mit Schadsoftware infizierte Computer, die von Kriminellen ferngesteuert und beispielsweise für Spam-Versand und für Attacken auf andere Computer missbraucht werden. Auf diese Weise „gekaperte" Computer können vom Nutzer unbemerkt auf ferngesteuerte Befehle von Kriminellen reagieren und zum Beispiel Spam versenden oder Attacken auf fremde Websites vornehmen.

Cyber Mobbing
Mit den aus dem Englischen kommenden Begriffen Cyber-Mobbing, auch Internet-Mobbing, Cyber-Bullying sowie Cyber-Stalking werden verschiedene Formen der Diffamierung, Belästigung, Bedrängung und Nötigung anderer Menschen oder Firmen mit Hilfe elektronischer Kommunikationsmittel über das Internet, in Chatrooms, beim Instant Messaging und/oder auch mittels Mobiltelefonen bezeichnet. Dazu gehört auch der Diebstahl von (virtuellen) Identitäten, um in fremden Namen Beleidigungen auszustoßen oder Geschäfte zu tätigen usw.
Opfer werden durch Bloßstellung im Internet, permanente Belästigung oder durch Verbreitung falscher Behauptungen gemobbt. Die Täter werden in diesem Zusammenhang auch als Bullies bezeichnet.

Firewall
Eine Firewall (besser mit Sicherheits-Gateway bezeichnet) ist ein System aus Soft-und Hardware-Komponenten, um IP-Netze sicher zu koppeln.

Hacking
Ein Fremder verschafft sich Zugang zu einem Computersystem ohne notwendige Autorisierung durch den Nutzer oder den Eigentümer

Man-in-the-Middle Attacke
Ziel bei einem Man-in-the-Middle-Angriff ist es, sich unbemerkt in eine Kommunikation zwischen zwei oder mehr Partnern einzuschleichen, beispielsweise um Informationen mitzulesen oder zu manipulieren. Hierbei begibt sich der Angreifer „in die Mitte" der Kommunikation, indem er sich gegenüber dem Sender als Empfänger und gegenüber dem Empfänger als Sender ausgibt. Gelingt es dem Angreifer, erfolgreich in die Kommunikation einzudringen, kann er evtl. sämtliche gesendeten Informationen, einsehen oder auch manipulieren, bevor er sie an den richtigen Empfänger weiterleitet.

Pharming
ist ein Betrugsmethode, die durch das Internet verbreitet wird. Sie basiert auf einer Manipulation der DNS-Anfragen von Webbrowsern (beispielsweise durch DNS-Spoofing), um den Benutzer auf gefälschte Webseiten umzuleiten. Es ist eine Weiterentwicklung des klassischen Phishings.

Phishing
Mit Phishing werden Versuche bezeichnet, über gefälschte Webseiten, E-Mails oder Kurznachrichten an persönliche Daten eines Internet-Benutzers zu gelangen. Mit den erhaltenen Daten werden beispielsweise Kontoplünderung begangen. Es handelt sich dabei um eine Form des Social Engineering, bei dem die Gutgläubigkeit des Opfers ausgenutzt wird. Der Begriff ist ein englisches Kunstwort, das sich an „fishing" (angeln, fischen) anlehnt.
So kann der Täter beispielsweise eine E-Mail versenden, die so aussieht, als käme sie von der Sparkasse des Opfers. Darin wird das Opfer unter einem Vorwand aufgefordert, sich auf der Seite der Sparkasse einzuloggen. Klickt das Opfer auf den in der E-Mail befindlichen Link, so gelangt er auf eine Seite des Täters, die aber so aussieht, als sei es die Seite der Sparkasse. Sobald das Opfer sich nun hier „bei seiner Sparkasse" einloggt, verfügt der Täter über die Anmeldedaten und kann ggf. das Konto des Opfers plündern.

Früher waren Phishing-Versuche leicht zu erkennen, da sie in schlechtem Deutsch geschrieben waren und Logos oder ähnliches nicht richtig nachgemacht dargestellt wurden. Inzwischen sind die Täuschungs-Versuche so raffiniert geworden, dass die Phishing-Mail äußerlich nicht von einer echten Mail zu unterscheiden ist.

Skimming
(engl. für „Abschöpfen") ist ein englischer Begriff für einen Man-in-the-middle-Angriff, der illegal die Daten von Kreditkarten oder Bankkarten ausspäht. Meist werden dabei an echten, aber heimlich präparierten Geldautomaten die Kartendaten ausgelesen und die PIN abgegriffen.

Spam
Missbrauch von elektronischen Sendediensten (z. B. E-Mails, SMS) zum Versand von nicht erwünschten und unaufgeforderten Massennachrichten, die entweder Werbung für dubiose Produkte enthält oder versucht, zum Beispiel über einen Link oder einen Anhang Schadsoftware zu installieren.

Trojanisches Pferd (Trojaner)
Programm, welches sich als nützliches Werkzeug tarnt, jedoch schädlichen Programmcode einschleust und im Verborgenen unerwünschte Aktionen ausführt.

Virenschutzprogramm
Ein Virenschutzprogramm ist eine Software, die bekannte Computer-Viren, Computer-Würmer und Trojanische Pferde aufspürt, blockiert und gegebenenfalls beseitigt.

Virus
Ein Computer-Virus ist eine Schadsoftware, die sich nach ihrer Ausführung selbst reproduziert und dadurch vom Anwender nicht kontrollierbare Manipulationen am System vornimmt.

Wurm
Ein Computer-Virus, der sich auch ohne Ausführung selbst reproduziert und sich im System (vor allem in Netzen) ausbreitet.

Ransomware (Erpressungssoftware)
Hierbei handelt es sich um eine Schadsoftware, die den Nutzer von seinen Daten aussperrt und dann ein Lösegeld fordert, um den Zugang wieder freizugeben.
In einfacheren Varianten (z. Bsp. der bekannte „BKA-Trojaner") wird lediglich der Systemstart manipuliert, so dass der Nutzer immer ein entsprechendes Hinweisfenster im Vordergrund hatte. Diese Manipulation lässt sich mit entsprechendem technischen Wissen rückgängig machen. In neueren Varianten werden unbemerkt wichtige persönliche Daten des Opfers verschlüsselt. Oftmals arbeitet diese Ransomware wochenlang im Hintergrund. Auf diese Weise sorgen die Kriminellen dafür, dass auch Sicherungskopien, die sich nur auf gelegentlich angeschlossenen Datenträgern (wie etwa einer externen Festplatte) befinden, verschlüsselt werden.
Zu einem festgelegten Zeitpunkt sperrt die Ransom-Ware dann den Zugriff auf die Daten, beispielsweise auf alle privaten Bilder des Opfers. Die Daten sind physisch zwar noch vorhanden, allerdings verschlüsselt. Dies betrifft dann auch die Datenträger mit den Sicherungskopien, die in der Zwischenzeit angeschlossen worden sind. Die Ransom-Ware verlangt die Zahlung eines bestimmten Geldbetrages, damit der Entschlüsselungscode übermittelt wird. Oft wird nach einer Zahlung nicht der Code übermittelt, sondern nur eine neue Zahlung verlangt. Sofern es sich um eine ausreichend starke Verschlüsselung handelt, gibt es sogar für Spezialisten keine technische Möglichkeit, die Daten zu entschlüsseln - sie bleiben ohne den Entschlüsselungscode dauerhaft unlesbar und damit verloren. Vor diesen Angriffen kann man sich darum nur vorsorgend schützen - so sollten zum Beispiel keinerlei verdächtigen Links angeklickt oder verdächtige Anhänge geöffnet werden. Dies betrifft sogar Links oder Anhänge von bekannten Absendern, da die Täter sich teilweise Zugang zu den E-Mails von Privatpersonen verschaffen und dann von dort heraus an alle im Adressbuch hinterlegten Kontakte den Link bzw. Anhang mit der Schadsoftware versenden.

Keylogger
Als Keylogger wird Hard- oder Software zum Mitschneiden von Tastatureingaben bezeichnet. Sie zeichnen alle Tastatureingaben auf, um sie möglichst unbemerkt an einen Angreifer zu übermitteln. Dieser kann dann aus diesen Informationen für ihn wichtige Daten, wie z. B. Anmeldeinformationen oder Kreditkartennummern, filtern.

Stand: 04/2016