Online?
Aber sicher!

Unsere Empfehlung für Ihre Online-Sicherheit

Niedersächsisches Ministerium
für Inneres und Sport

Liebe Mitbürgerinnen und Mitbürger,

Digitalisierung ist für uns alle längst kein abstraktes, theoretisches Thema mehr. Ganz im Gegenteil. Wir alle werden täglich mit den Chancen und Risiken des digital geprägten Lebens und Arbeitens konfrontiert. Dabei kann die Bedeutung der Cybersicherheit gar nicht hoch genug eingeschätzt werden. Diese Sicherheit der Netze, der Rechner und der mobilen Endgeräte ist ein zentraler Baustein für das Leben im digitalen Zeitalter.

Darum ist es mir sehr wichtig, die Menschen in Niedersachsen für dieses Thema immer wieder und auf allen möglichen Wegen und über verschiedene Plattformen dafür zu sensibilisieren. Das ist die Grundlage dafür, sich sicher und souverän in der digitalen Welt bewegen zu können. Wir müssen uns darüber bewusst sein, dass im Grunde jede und jeder 24 Stunden am Tag digital angreifbar ist. Ob es sich um Unternehmen, Verwaltungsbehörden, Kritische Infrastrukturen für die Daseinsvorsorge, Sicherheitsbehörden oder auch private Computer oder Smartphones handelt: Alle können Opfer von Cyberangriffen werden. Nahezu täglich erreichen uns Meldungen über die unterschiedlichen Maschen von Cyberkriminellen und anderen Akteuren, die an unsere Daten, an unsere Identitäten oder an unser Geld kommen wollen. Wenn wir uns in der digitalen Welt bewegen, dann ist es wichtig zu wissen, worauf es ankommt und mit welchen Mitteln wir uns schützen können.

Wir müssen verinnerlichen, mit unseren digitalen Daten genauso umzugehen, wie wir das in der analogen Welt ganz selbstverständlich tun. Zuhause schließen wir die Tür ab, wir lassen ein Auto nicht unabgeschlossen stehen und wir wissen, dass die PIN nicht als Notiz auf die EC-Karte oder Kreditkarte gehört. Genauso selbstverständlich muss es sein, ein paar Grundregeln zu beachten, wenn wir in der Cyberwelt unterwegs sind. Nur so können die vielfältigen Angebote und Möglichkeiten der digitalen Welt souverän genutzt werden, ohne gleich in die erstbeste Falle zu tappen.Diese Broschüre dient Ihnen als kleine Orientierung, mit welchen grundlegenden Maßnahmen oder Verhaltensweisen Sie sich noch besser schützen können, durch welche Stellen Sie sich weiter informieren können und was Sie unternehmen sollten, wenn Sie doch Opfer eines Hackers geworden sind.

Gehen Sie Online, aber sicher!

Ihr

Boris Pistorius
Niedersächsischer Minister
für Inneres und Sport

Niedersachsen

Eine Broschüre, viele Antworten.

| Wie schütze ich mich vor Hackerangriffen?

| Wie sichere ich mein Smartphone vor unbefugten Zugriffen?

| Wie bleiben meine Daten auch wirklich mein Eigentum?

Von Alexa bis zur Zahnbürste: Immer mehr Geräte des täglichen Lebens sind vernetzt. Das erleichtert oft den Alltag, es geraten dadurch aber auch massenweise – teils sensible – persönliche Daten in den digitalen Raum. Das Niedersächsische Ministerium für Inneres und Sport möchte Sie für diese Risiken sensibilisieren. Ziel ist es, die digitale Souveränität und informationelle Selbstbestimmung zu stärken. Diese Broschüre bietet Ihnen wichtige Tipps zu grundlegenden Schutz- und Sicherheitsmaßnahmen. Eine kleine Übersicht zu weiteren Informationsquellen und Unterstützungsangeboten gibt Orientierung zur Vertiefung oder auch für Opfer von Hackern.

Verständlich, anschaulich und praxisorientiert.

Die 12 wichtigsten Sicherheitsmaßnahmen

1. Aktuelle Anti-Viren-Software

Natürlich ist eine kostenlose Anti-Viren-Software besser als keine, und insbesondere der bei Microsoft Windows eingebaute „Windows Defender" bietet guten Schutz. Der Einsatz von kostenpflichtigen Schutzprogrammen bringt jedoch oft zusätzlichen Schutz durch weitere Funktionen und Vorteile, die den kostenlosen Versionen vielfach fehlt.

2. Aktuelles Betriebssystem mit aktuellen Updates

Nutzen Sie, wenn möglich das neuste Betriebssystem, ob nun Microsoft Windows, Apple Mac OSx, iOS, Android oder ein Linux-Betriebssystem und halten Sie dieses stets auf dem neusten Stand. Regelmäßige Updates und Patches sind unerlässlich. Am besten sollten Sie die automatische Aktualisierung der Systeme eingestellt haben. Dies gilt auch für alle anderen Anwendungen, wie z. B. Office-Programmen oder auch Browsern (z. B. Chrome, Safari, Internet Explorer/Edge oder Firefox).

3. Aktivierte Firewall

Die Firewall kann unter Umständen als „lästig" empfunden werden sein. Für Ihre Sicherheit ist eine effektive Firewall aber unerlässlich. Deaktivieren Sie die Firewall, daher auf keinen Fall. Auch nicht, um dadurch wiederkehrenden Meldungen aus dem Weg zu gehen.

4. Regelmäßige „Offline“-Backups

Führen Sie regelmäßig „Offline“-Backups durch, indem Sie eine externe Festplatte anschließen und die Daten darauf sichern. Anschließend entfernen Sie die Festplatte vom Computer (Offline) und lagern diese an einem sicheren Ort. Bei Bedarf können Sie die Daten nach einer neuen Installation des Computers wieder herüberspielen. Diese Daten sollten vor der erneuten Nutzung vorsichtshalber auf Schadsoftware geprüft werden.

5. Hinterfragen des E-Mail-Inhalts sowie der Absenderinformation

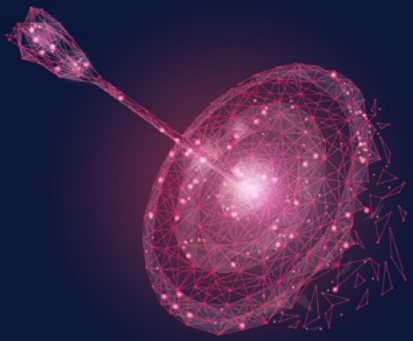
Hinterfragen Sie den Inhalt erhaltener E-Mails auf Sinnhaftigkeit. Prüfen Sie, ob der Inhalt plausibel ist. Achten Sie auch auf typische Merkmale von potentiell gefährlichen E-Mails, wie falsche Absender-Adresse, Uhrzeit des E-Mail-Eingangs, Schreib- und Grammatikfehler oder z.B. ein Fehler in der Signatur.

6. Prüfen von E-Mail-Anhängen hinsichtlich des Datenformats

Nicht jeder Anhang muss pauschal gefährlich sein. Insbesondere bei „.exe“-Formaten und Ihnen nicht bekannten Datei-Formaten ist jedoch größte Vorsicht geboten! Auch bei .zip und .doc Dateien ist Ihre Wachsamkeit wichtig!

Im Zweifel löschen Sie die E-Mail. Wenden Sie sich für weitere Informationen bzw. zur Prüfung der E-Mail an Ihren Administrator – allerdings OHNE den verdächtigen Inhalt zu öffnen oder weiterzuleiten!

7. Prüfen des Ziels eines Links in einer E-Mail



Links leiten Sie meistens auf Webseiten weiter. Dort erhalten Sie, wenn die Nachricht von einem Angreifer kommt, höchstwahrscheinlich einen Schadcode, der Ihrem Computer und Ihren Daten großen Schaden zufügen kann. Prüfen Sie das Ziel des Links, indem Sie mit der Maus über den Link fahren (Mouse-over). Sehen Sie Unterschiede im Domänen-Namen, sollten Sie den Link nicht öffnen und die E-Mail löschen. Beispiel: grnail.com ist nicht gmail.com oder goog1e.de ist nicht google.de!

8. Einsatz komplexer Passwörter

- Hohe Komplexität
  - min. 10 Zeichen
  - Groß- und Kleinbuchstaben, Sonderzeichen, Zahlen
- Geheimhaltung
- Unterschiedliche Kennwörter
- Passwort-Safes für allgemeine Passworte (Nicht für sensible Zwecke)

9. Einsatz von Zwei-Faktor-Authentifizierung

Wie seit September 2019 durch Banken gefordert, wird eine Zwei-Faktor-Authentifizierung auch von vielen Anbietern (wie z. B. eBay, Amazon oder PayPal etc.) im Internet angeboten. Eine Anleitung und Aktivierung der Funktion findet man in der Regel in den Sicherheitseinstellungen des jeweiligen Anbieters.

10. Aktivieren Sie auch die „Firewall im Kopf“

Hinterfragen Sie stets Ihr Handeln im Umgang mit E-Mails und dem Internet und seien Sie aufmerksam. Nicht jeder Online-Shop ist seriös, nur weil er eine augenscheinlich sichere Webseite anbietet. Phishing-E-Mails und Webseiten erscheinen dem Original täuschend echt. Aber würde eine Bank wirklich sensible Daten per E-Mail anfordern? Ist Ihre Kreditkarte für Sicherheitseinstellung eines Webshops notwendig? Wohl kaum.

11. Alle Maßnahmen gelten auch für den Smartphone-Einsatz

Betrachten Sie Ihr Smartphone als einen Computer in der Hosen- oder Handtasche. Angriffe sind auf einem Smartphone längst gängige Praxis der Angreifer. Mehr noch, Ihr Smartphone ist ständig online, Ihr Laptop wahrscheinlich nicht. Somit gelten die genannten Maßnahmen auch für Smartphones. Zudem ist der Einsatz in öffentlichen Hotspots mit Risiken verbunden. Auch hier ist Vorsicht geboten. Nutzen Sie öffentliches WLAN am Smartphone nur bei Bedarf.

12. Angriffsziel Mensch

Immer mehr Angreifer versuchen durch manipulative Techniken, den Anwender direkt zu Handlungen für Ihre Zwecke zu verleiten. Oft nutzen die Angreifer die Hilfsbereitschaft aus, bauen ein Vertrauensverhältnis auf oder erzeugen gezielt Druck bei den Anwendern, um dadurch an sensible Informationen zu gelangen. Seien Sie sparsam mit Informationen und geben Sie diese nicht an Ihnen unbekannter Personen weiter.

Weitere Informationsangebote

Bundesamt für Sicherheit in der Informationstechnik

Das Bundesamt für Sicherheit in der Informationstechnik gestaltet als die Cybersicherheitsbehörde des Bundes Informationssicherheit in der Digitalisierung durch Prävention, Detektion und Reaktion für Staat, Wirtschaft und Gesellschaft. Das Nationale Verbindungswesen des BSI stellt an regionalen Ballungsräumen Ansprechpartner zur Verfügung, die vor Ort Fragen rund um das BSI und Cyber-Sicherheit beantworten.

BSIregional@bsi.bund.de
www.bsi.bund.de

Niedersächsisches Ministerium für Inneres und Sport
Verfassungsschutz

Der Arbeitsbereich Wirtschaftsschutz des niedersächsischen Verfassungsschutzes ist ein Partner für die Wirtschaft - neutraler Dienstleister und losgelöst vom Strafverfolgungszwang! Wir bieten Beratungen und Vortragsinhalte: Wirtschafts- und Industriespionage, Cybersicherheit, Know-how-Schutz, Industrie 4.0, Sicherheit in der Informations- und Kommunikationstechnologie, Geheimschutz in der Wirtschaft, Sicherheit auf Geschäftsreisen im Ausland, Innentäterproblematik und Social Engineering.

www.verfassungsschutz.niedersachsen.de

LANDESKRIMINALAMT NIEDERSACHSEN

Über den Ratgeber Internetkriminalität der Polizei Niedersachsen auf **www.polizei-praevention.de** können Sie sich offiziell, aktuell und zuverlässig über Gefahren im Internet informieren, wichtige Tipps gegen Cybercrime erfahren und auch vertraulich Ihre persönlichen Fragen stellen.

KINDERSCHUTZALLIANZ
THE ALLIANCE FOR CHILDREN

Die KINDERSCHUTZALLIANZ hat sich zum Ziel gesetzt, nachhaltige Lösungen zur Bekämpfung von sexualisierter Gewalt gegen Kinder und Jugendliche in der digitalen und nicht-digitalen Welt zu schaffen. In diesem weltweit einzigartigen Bündnis engagieren sich unterschiedliche Organisationen aus Gesellschaft, Politik, Wirtschaft und Verwaltung. Das Niedersächsische Ministerium für Inneres und Sport stellt die Geschäftsstelle des Bündnisses.

+49 (0) 511 120-4780
info@kischaz.de
www.kinderschutzallianz.org

Die Zentralen Ansprechstellen Cybercrime für die Wirtschaft (ZAC) wurden 2010 in jedem Bundesland eingerichtet und dienen als Single Point of Contact für die Wirtschaft, Behörden und Verbände. In Niedersachsen werden darüber hinaus konkrete Maßnahmen zur Vermeidung von Cyberangriffen im Rahmen von Vorträgen und Beratungen vor Ort sowie mit Hilfe von Checklisten auf der umfangreichen Webseite vermittelt. Im Falle eines Cyberangriffs koordiniert die ZAC die wichtigen Sofortmaßnahmen und steht als erster polizeilicher Ansprechpartner zur Verfügung.

+49 (0) 511 26262-3804
zac@lka.polizei.niedersachsen.de
www.zac-niedersachsen.de

klicksafe ist eine Sensibilisierungskampagne zur Förderung der Medienkompetenz im Umgang mit dem Internet und neuen Medien im Auftrag der Europäischen Kommission.

Auf der Webseite **www.klicksafe.de** finden Sie eine Vielzahl von aktuellen Informationen, praktischen Tipps und Unterrichtsmaterial zu digitalen Diensten und Themen.

Weitere Informationsangebote

JUUUPORT.de ist eine bundesweite Online-Beratungsplattform, an die Du Dich wenden kannst, wenn Du Probleme im Netz hast, z.B. gemobbt oder abgezockt wurdest. Hier bekommst Du Hilfe von Jugendlichen, den JUUUPORT-Scouts. Ihre Beratung ist anonym und kostenlos.

Ansprechpartner sind die JUUUPORT.de Scouts unter www.JUUUPORT.de

Deutschland sicher im Netz e.V. bietet mit dem Projekt PolisiN kostenlose und bedarfsgerechte Workshops an: für Politiker*innen und Mitarbeiter*innen in Partei, Fraktion und Büros, auf Bundes-, Landes- und kommunaler Ebene. PolisiN schult zu Themen wie Accountsicherheit, Phishing und Datensicherheit im Netz und geht auf eigene Themenvorschläge ein.

info@sicher-im-netz.de
www.polisin.de

Mit dem Projekt Digitale Nachbarschaft (DiNa) sensibilisiert Deutschland sicher im Netz e.V. Vereine, Initiativen und freiwillig engagierte Bürger*innen für die Chancen der Digitalisierung. Das Projekt verfügt über ein bundesweites Netzwerk von 50 regionalen Anlaufstellen (DiNa-Treffs), das bedarfsgerechte Unterstützungsangebote für Bürger*innen im Ehrenamt bereitstellt. Mit zwei Infobussen (DiNa-Mobile) ist die DiNa auch mobil im Einsatz zu Fragen der Digitalisierung.

+49 (0) 30 27576-370
dina@digitale-nachbarschaft.de
www.digitale-nachbarschaft.de

verbraucherzentrale
Niedersachsen

Die Verbraucherzentrale Niedersachsen e. V. berät individuell und anbieterunabhängig zu vielen Fragen, die für Verbraucher*innen wichtig sind. Hierzu zählen die Themenbereiche Internet und Telefon, Verbraucherrecht, Finanzen, Versicherungen, Gesundheit, Energie und Bauen sowie Rundfunkbeiträge.

+49 (0) 511-91196-0
info@verbraucherzentrale-niedersachsen.de
www.verbraucherzentrale-niedersachsen.de

WEISSER RING
Wir helfen Kriminalitätsopfern.

Der WEISSE RING e.V. hilft Menschen, die Opfer von Kriminalität und Gewalt geworden sind. Wir tun dies als gemeinnütziger und einziger bundesweit tätiger Opferhilfeverein mit rund 2.900 ehrenamtlichen, professionell ausgebildeten Helfern in mehr als 400 Außenstellen, dem Opfer-Telefon und der Onlineberatung. Unsere Opferhelfer kennen die Rechte von Betroffenen und wissen, welche Leistungen möglich sind. Sie sind vielfach vernetzt und vermitteln bei Bedarf schnell und direkt den Zugang zu Experten oder Hilfsleistungen anderer Organisationen.

+49 (0) 6131 83 03-0
Opfer-Telefon 116 006
www.weisser-ring.de

Impressum / Herausgeber:

Niedersächsisches Ministerium für Inneres und Sport
Lavesallee 6
30169 Hannover

www.mi.niedersachsen.de

Stand: März 2021

Niedersächsisches Ministerium
für Inneres und Sport