

## **DAS INTERNET SICHER NUTZEN**

**Lieber Kunde,**

herzlich Willkommen im lichtschnellen Glasfasernetz der Gemeindewerke Hohenwestedt.

Dieses Dokument bietet Ihnen zehn hilfreiche Tipps zur sicheren Nutzung des Internets, um Risiken wie Schadsoftware und Identitätsdiebstahl zu vermeiden.

### **1. Sicheres Einrichten und Aktualisieren des Webbrowsers**

Um sicher im Internet zu surfen, ist es wichtig, den Webbrowser sicher einzurichten und regelmäßig zu aktualisieren. Dies reduziert das Risiko von Sicherheitslücken und schützt vor Schadsoftware.

- Deaktivieren oder deinstallieren Sie unnötige Browser-Erweiterungen.
- Halten Sie den Browser stets auf dem neuesten Stand, um Sicherheitslücken zu schließen.
- Nutzen Sie Programme zum Blockieren von Werbung, um sich vor Malvertising zu schützen.
- Geben Sie sicherheitskritische Webseiten manuell ein und speichern Sie diese als Lesezeichen.

### **2. Aktuelle Software und Betriebssysteme verwenden**

Die Verwendung aktueller Software und Betriebssysteme ist entscheidend für die Sicherheit im Internet. Regelmäßige Updates schließen Sicherheitslücken und verringern das Risiko von Angriffen.

- Aktivieren Sie die automatische Aktualisierung für Betriebssysteme und Programme.
- Überprüfen Sie regelmäßig die Einstellungen unter Update, um sicherzustellen, dass alles aktuell ist.
- Deinstallieren Sie nicht mehr benötigte Programme, um die Angriffsfläche zu verringern.

### **3. Virenschutz und Firewall aktivieren**

Ein effektiver Virenschutz und eine aktivierte Firewall sind grundlegende Maßnahmen zum Schutz vor Cyberangriffen. Diese Tools sollten immer aktiviert sein, um die Sicherheit zu erhöhen.

- Nutzen Sie integrierte Virenschutz- und Firewall-Anwendungen in Ihrem Betriebssystem.
- Seien Sie sich bewusst, dass diese Maßnahmen nicht alle Risiken ausschließen können.
- Kombinieren Sie diese Maßnahmen mit anderen Sicherheitstipps für umfassenden Schutz.

### **4. Benutzerkonten mit eingeschränkten Rechten anlegen**

Die Einrichtung unterschiedlicher Benutzerkonten mit eingeschränkten Rechten schützt vor unbefugtem Zugriff auf persönliche Daten. Dies ist besonders wichtig, um Schadsoftware zu minimieren.

- Erstellen Sie passwortgeschützte Benutzerkonten für alle Nutzer des PCs.
- Arbeiten Sie nur mit Administratorrechten, wenn es unbedingt erforderlich ist.
- Schützen Sie private Dateien durch eingeschränkte Berechtigungen.

## **5. Sichere Passwörter für Online-Konten verwenden**

Sichere Passwörter sind entscheidend für den Schutz Ihrer Online- und Benutzerkonten.

Jedes Konto sollte ein einzigartiges, starkes Passwort haben.

- Verwenden Sie Passwörter mit mindestens acht Zeichen, die Groß- und Kleinbuchstaben, Ziffern und Sonderzeichen enthalten.
- Ändern Sie voreingestellte Passwörter nach der ersten Nutzung.
- Nutzen Sie, wo möglich, eine Zwei-Faktor-Authentifizierung zur zusätzlichen Sicherheit.

## **6. Vorsicht bei E-Mails und Anhängen walten lassen**

E-Mails können ein Einfallstor für Schadsoftware sein, daher ist Vorsicht geboten.

Überprüfen Sie Absender und Inhalte sorgfältig, bevor Sie Links oder Anhänge öffnen.

- Vermeiden Sie HTML-Format in E-Mails und nutzen Sie stattdessen reines Textformat.
- Seien Sie skeptisch bei unbekannten Absendern und ungewöhnlichen E-Mails von bekannten Kontakten.
- Achten Sie auf Merkmale wie fehlerhafte Schreibweise oder verdächtige Links.

## **7. Vorsicht beim Herunterladen von Programmen**

Das Herunterladen von Programmen birgt Risiken, insbesondere wenn die Quelle nicht vertrauenswürdig ist. Seien Sie vorsichtig und überprüfen Sie die Seriosität der Quelle.

- Laden Sie Programme vorzugsweise von den offiziellen Webseiten der Hersteller herunter.
- Nutzen Sie verschlüsselte Seiten (https) für Downloads.
- Recherchieren Sie über den Hersteller, um mehr Informationen zu erhalten.

## **8. Zurückhaltung bei der Weitergabe persönlicher Daten**

Die Weitergabe persönlicher Daten sollte mit Bedacht erfolgen, um Missbrauch zu vermeiden. Überlegen Sie, welchen Diensten Sie Ihre Daten anvertrauen.

- Vermeiden Sie die ungeschützte Weitergabe persönlicher Daten in offenen Netzwerken.
- Seien Sie vorsichtig bei der Eingabe persönlicher Daten auf Webseiten.

## **9. Daten durch Verschlüsselung schützen**

Die Verschlüsselung von Daten ist ein wichtiger Schritt zum Schutz Ihrer persönlichen Informationen. Achten Sie darauf, nur auf sicheren Webseiten persönliche Daten einzugeben.

- Nutzen Sie Webseiten mit https für die Eingabe vertraulicher Informationen.
- Verschlüsseln Sie auch E-Mails, wenn möglich.
- Achten Sie auf die Verschlüsselung Ihres WLANs und verwenden Sie WPA2 oder WPA3.

## **10. Regelmäßige Sicherheitskopien anfertigen**

Regelmäßige Backups sind entscheidend, um Datenverluste zu vermeiden. Diese sollten auf externen Speichermedien oder in der Cloud gesichert werden.

- Erstellen Sie Sicherungskopien Ihrer Dateien auf externen Festplatten oder USB-Sticks.
- Stellen Sie nur Daten aus Sicherungskopien wieder her, keine Programme.
- Halten Sie Datenträger nur bei Bedarf mit dem PC verbunden, um das Risiko zu minimieren.

Wir hoffen, dass wir Ihnen mit diesen Tipps helfen konnten und wünschen Ihnen viel Spaß mit Ihrem lichtschnellem Glasfaseranschluss der Gemeindewerke Hohenwestedt.