Novak Renata, IKT

Stand 9/2020

Orientierungshilfe

Cybersicherheit im Home Office

Allgemeine Information

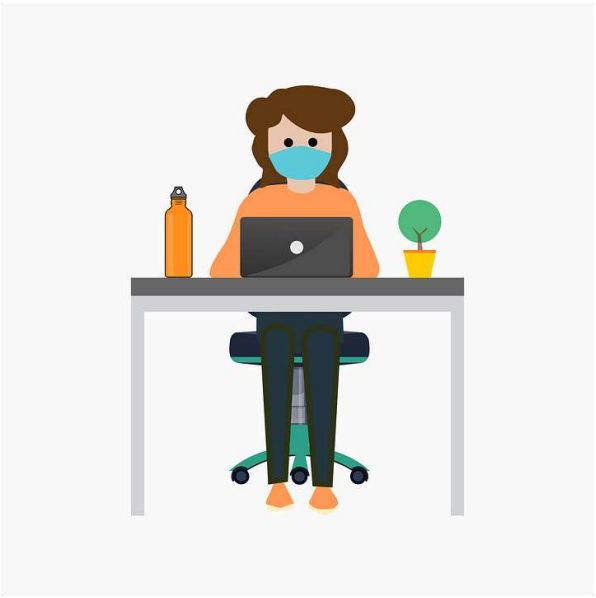
In dieser Orientierungshilfe sind Empfehlungen zusammengefasst worden, um den Home Office Arbeitsplatz sicherer zu gestalten.

Beim Arbeiten im HB sind die Firmendaten im eigenem Netzwerk geschützt.

Für das Home Office bietet das HB die Möglichkeit an, über das Portal bequem in das Firmennetzwerk einzusteigen.

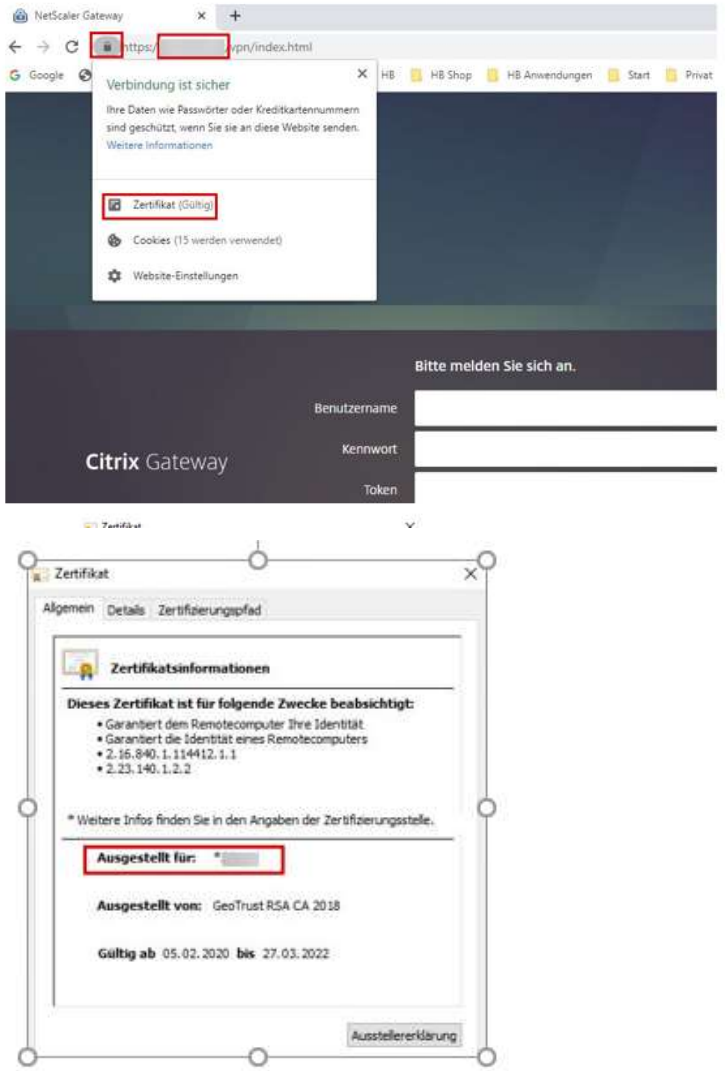
Wir legen jedem Home Office Mitarbeiter die Empfehlungen ans Herz, egal ob Sie ein Firmengerät zur Verfügung gestellt bekommen haben oder auf einem Privatgerät arbeiten.

Wenn Sie Firmengeräte von HB zur Verfügung gestellt bekommen haben, dann sind diese Geräte sicherheitstechnisch auf dem neuesten Stand.



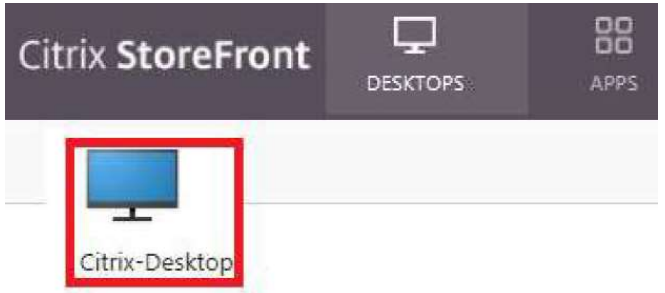
Portal – Citrix Anmeldung über Token

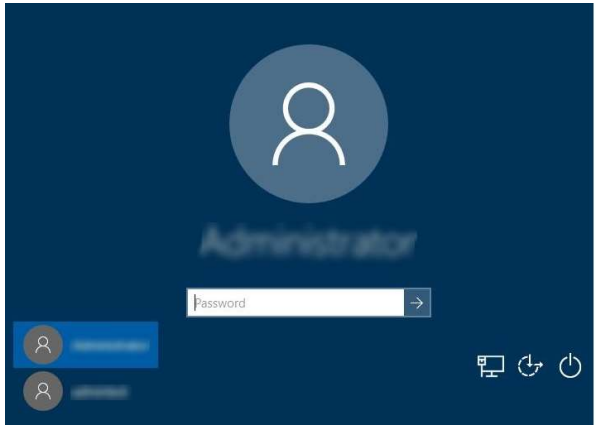
- Um auf das Firmennetzwerk zugreifen zu können, tragen Sie im Internet Browser (Chrome) den Namen der Portalseite ein. Weitere Infos erhalten Sie bei der IKT.
- Gleich links neben der Adresse ist ein Schlüssel-Symbol zu sehen.
- Das Symbol bedeutet, dass die Verbindung sicher ist.
- Klickt man auf das Schlüsselsymbol und dann auf Zertifikat, so wird das gültige Zertifikat angezeigt.
- Achtung: Bei einem roten Rufzeichen ist die Verbindung nicht sicher. "Nicht sicher" oder "Schädlich"



Cybersicherheit am Arbeitsgerät – Physische Sicherheit

- Stellen Sie sicher, dass Ihnen niemand beim Arbeiten auf Ihren Bildschirm blickt
- Wenn Sie vertrauliche Gespräche führen, dann achten Sie darauf, dass die Kommunikation von niemandem mitgehört werden kann
- Achten Sie darauf, dass niemand Zugriff auf Ihr Arbeitsgerät hat, während Sie eine offene Citrix Sitzung haben.
- Wenn Sie den Arbeitsplatz kurz verlassen, dann sperren Sie Ihr Arbeitsgerät
  Tipp: Tastenkürzel Windows-Taste + L
- Speichern Sie Ihre Daten nur in der Citrix Umgebung, d.h. speichern Sie Firmendaten nicht auf dem privatem Gerät ab.

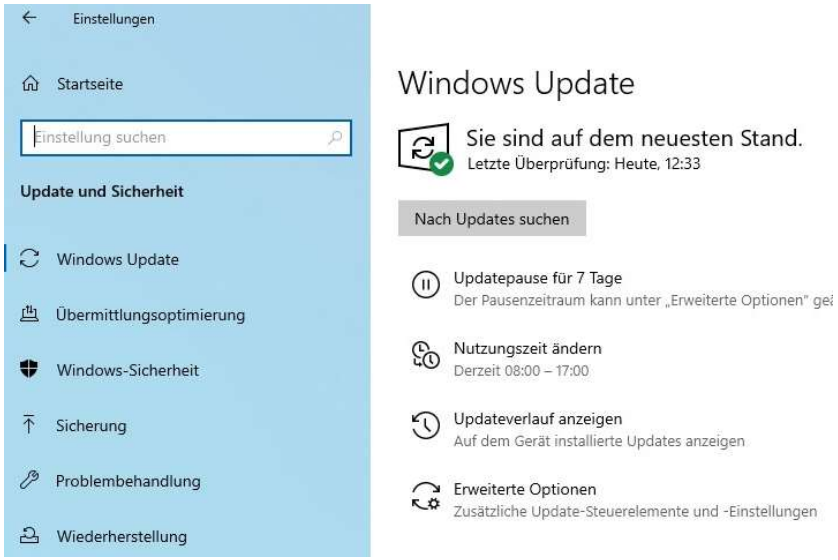




Cybersicherheit am Arbeitsgerät – Sicherheits-Updates

- Spielen Sie alle für Ihre Arbeitsgeräte verfügbaren Sicherheits-Updates gewissenhaft und zeitnah ein und starten Ihr Arbeitsgerät immer neu.

  Tipp: Unter Startmenü / Einstellungen / Update und Sicherheit sehen Sie, ob das Gerät auf dem neuesten Stand ist



- Deaktivieren Sie auf keinen Fall Funktionalitäten zum automatisierten Einspielen von Sicherheits-Updates.
- Schützen Sie Ihr Arbeitsgerät immer mit einem Antivirenprogramm.
- Halten Sie Ihr Antivirenprogramm immer auf dem aktuellen Stand
- Sichern Sie Ihr Gerät mit einer Firewall ab

Sicheres Verhalten

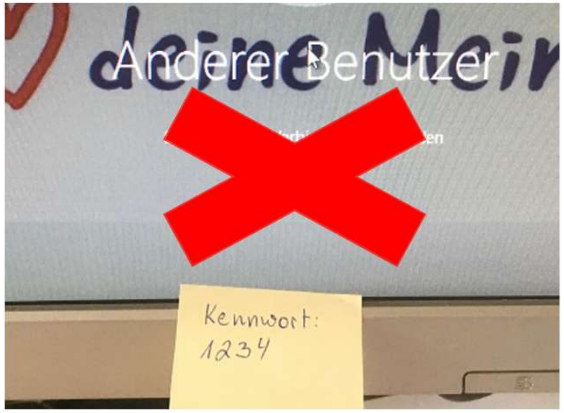
- Geben Sie Ihre persönlichen Zugangsdaten ausnahmslos niemanden weiter. Lassen Sie das Kennwort nie offen herumliegen

- Befolgen Sie niemals Anweisungen eines unbekannten Anrufers bzw. geben Sie niemals vertrauliche Daten an unbekannte Anrufer weiter

- Behandeln Sie Mails von unbekannten Absendern mit einem gesunden Maß an Skepsis.
  Achten Sie bei unerwarteten Mails auf die Schreibweise
  Beispiel: Richtig: max.meier@hb.at / Fälschung: max.meier@hbb.at

- Öffnen Sie keine fragwürdigen E-Mail-Anhänge und klicken Sie nicht auf Hyperlinks in E-Mails (Phishing-Mails)

- Schließen Sie keine unbekannten USB-Sticks an Ihr Arbeitsgerät



Beispiel für Phishing-Mail

Von:
Gesendet: Montag, 29. April 2019 04:29
An:
Betreff: 29.04.2019 offene Rechnung NR. 3289444

Sehr geehrter Kunde

es wurde festgestellt, dass unsere Zahlungsanforderung Nummer 3289444 immer noch nicht ausgeglichen wurde.

Wir geben Ihnen jedoch trotzdem noch eine letzte Chance, Ihre Verpflichtung zu erfüllen, indem Sie innerhalb von 5 Tagen die ausstehende Rechnung in Höhe von 426,00 EURO an uns zahlen.

Die Einzelheiten der Bestellung und die Bankdaten können Sie in Ihrem Warenkorb unter der Website ansehen.

Falls der Schuldbetrag nicht überwiesen wird, sind wir außerdem gesetzlich dazu verpflichtet Vollstreckungsmaßnahmen gegen Sie einzuleiten. Um Ihnen diese Unannehmlichkeit zu ersparen, sollten Sie die Rechnung umgehend zahlen.

beachten Sie, über die Verzinsung der Forderung hinaus hat der Schuldner auch jeden weiteren durch den Verzug entstandenen Schaden zu ersetzen.

GmbH
86316 Friedberg

USt-IdNr.: DE

Beispiel einer erfundenen Forderung per E-Mail: Ein hoher Rechnungsbetrag soll noch offen sein und der Empfänger soll auf einen Link klicken, um weitere Infos zu erhalten. Nicht anklicken! In der Datei befindet sich Schad-Software.

Quelle: https://www.verbraucherzentrale.de/wissen/digitale-welt/onlinehandel/erfundene-rechnungen-kommen-mit-echten-daten-per-email-35975

Weitere Informationen, Tipps, …

- *Vollständiger Beitrag vom Bundesministerium für Inneres*
  https://www.bvt.gv.at/401/files/CSC/CSC_Schriftenreihe_Cyber_Sicherheit_im_Home_Office_Juli_2020_BF_20200727.pdf
- *Infos: Beschreibung zur Token Anmeldung*
  ..\..\..\..\..\..\Allgemeines\Information\Infra IKT\Citrix Anmeldung per Token.pdf
- *Infos: Umfassender Schutz mit Windows-Sicherheit*
  https://support.microsoft.com/de-at/help/4013263/windows-10-stay-protected-with-windows-security#
- *Tipps zu Antivirenprogrammen*
  https://www.heise.de/security/artikel/Der-richtige-Virenschutz-1105416.html?seite=2