POLIZEI
Nordrhein-Westfalen
Landeskriminalamt

bürgerorientiert • professionell • rechtsstaatlich

HÖHERE ONLINE-RISIKEN DURCH COVID-19
Verhaltenshinweise für Teilnehmende am Homeoffice sowie für Lehrkräfte, Eltern, Kinder und Jugendliche im Distanzunterricht

Allgemeine Hinweise

> Die Corona-Pandemie greift tief in das Leben der Menschen ein: Arbeiten von zu Hause, Lernen zu Hause, Freizeitgestaltung zu Hause.
In einigen Weltregionen ist lt. Unicef[1] die Internetnutzung seither um 50 Prozent gestiegen. Nicht alle haben das Wissen, die Ressourcen und die Kompetenzen, sich angemessen vor Online-Risiken zu schützen.

Homeoffice

> Regelmäßige Videokonferenzen können einen intimen Einblick in den eigenen Wohnbereich gestatten. Unbewusst wird die persönliche Wohnsituation mit allen Teilnehmenden geteilt, aber auch unbeabsichtigtes Auftreten von nicht beteiligten Personen im Hintergrund ist möglich. Zusätzlich lassen sich diese Videokonferenzen per Screenshot oder Videomitschnitt problemlos speichern und können somit an unberechtigte Dritte weitergegeben oder sogar auf Videoplattformen veröffentlicht werden. Alle Nutzerinnen und Nutzer digitaler Lernmethoden sollten sich über die Möglichkeiten, aber auch die Gefahren von virtuellen Klassenzimmern, digitaler Kommunikation und Online-Bildungsangeboten informieren.

Digitaler Unterricht

> Die andauernde Corona-Pandemie und die damit verbundene Schließung von Schulen hat Schülerinnen und Schüler, Eltern, Lehrkräften, Schulleitungen sowie die Bildungsadministration vor bisher unbekannte Herausforderungen gestellt, denen alle Beteiligte mit erheblichem Engagement begegnet sind. Cyberkriminalität kann in die privaten Bereiche von Lehrerinnen und Lehrern, Eltern, Schülerinnen und Schülern vordringen. Kinder und Jugendliche nutzen ggf. ihre Rechner, Laptops, Tablets und Handys zum ersten Mal für Aufgaben im schulischen Bereich. Sie legen sich neue E-Mailadressen an, installieren unbekannte Software, bewegen sich auf ganz unterschiedlichen Webseiten und setzen sich z. B. der Gefahr aus, Malware zu laden.

> Nicht nur im Homeoffice kommen Videochats zum Einsatz. Auch Schulen nutzen diese Tools, damit

[1] https://www.unicef.de/informieren/aktuelles/presse/2020/online-risiken-fuer-kinder-durch-covid-19/214286

Kontakt:
Landeskriminalamt Nordrhein-Westfalen
Völklinger Straße 49
40221 Düsseldorf

Stand: Februar 2021

Lehrkräfte in Kontakt mit den Schülerinnen und Schülern bleiben. Leider nutzen das einige derzeit aus, dass sich noch nicht alle mit diesen Programmen eingearbeitet haben und dringen unerwünscht in Videokonferenzen ein (sog. „Zoombombing“).

> Dieses Problem besteht nicht exklusiv bei einem, sondern bei allen Videokonferenzsystemen, die nicht auf eine geschlossene Nutzergruppe beschränkt sind. In sozialen Medien werden Anleitungen versandt, wie Unterrichtseinheiten „gecrasht“ werden können. Dabei werden immer dieselben Methoden angewandt:
    - Der Zugangslink und/oder die Einwahldaten werden versandt/weitergegeben.
    - Die eigentlichen Administratoren vergeben die falschen Rollen (ein Teilnehmder sollte nie als Moderator/Host eingetragen sein).
    - Die Teilnehmenden haben keine vorher festgelegten Namen und der Zugang wird nicht über einen Warteraum reguliert.

Verhaltenshinweise

> Um zu verhindern, dass Unbekannte Unterrichtsstunden stören, sollte man sich die Sicherheitseinstellungen der verwendeten Software genau ansehen und diese möglichst restriktiv konfigurieren.

> Empfohlene Sicherheitseinstellungen für einen virtuellen Konferenzraum:
    - Er kann nicht vor/ohne Anwesenheit des Erstellenden betreten werden.
    - Die Funktion “Warteraum bzw. Lobby“ aktivieren, über die der Erstellende die Teilnehmenden manuell in das Meeting einlassen muss.

> Da bei Weitergabe von Link und Passwort Außenstehende sich unter falschem Namen Zutritt verschaffen können, sollte man sich vorab ansehen, wie man solche ungebetene Gäste schnell ausschließen kann.

> Die Lehrkraft sollte zudem nach Ende der Unterrichtseinheit die Konferenz nicht einfach verlassen, sondern sie beenden, damit die Schülerinnen und Schüler nicht unbeaufsichtigt im Raum bleiben.

Weitere Sicherheitsmaßnahmen

Vorbemerkung: Die Gefahr des Cybermobbing endet nicht mit dem Schulschluss. Der Einblick in das persönliche Wohnumfeld, der ansonsten selten gewährt wird, zeigt intime Details wie z. B. Fotografien oder die Wohneinrichtung auf. Im Livestream getätigte Aussagen oder körperliche Übungen im Online-Sportunterricht können Anlass zum Mobbing geben.

> Achten Sie bei der Positionierung der Kamera darauf, dass möglichst wenig Details Ihrer Wohnung sichtbar sind. Nutzen Sie ggf. die Möglichkeit eines virtuellen Hintergrundes. Informieren Sie anwesende Personen über die Videokonferenz.

> Machen Sie sich bewusst, dass im Livestream getätigte Aussagen oder Handlungen eventuell unberechtigt aufgezeichnet werden können.

> Machen Sie vor Beginn eines Online-Unterrichtes deutlich, dass Aufnahmen von Bild und Ton untersagt sind und auch strafrechtliche Konsequenzen nach sich ziehen können. In diesem Zusammenhang sind sich viele Kinder und Jugendliche gar nicht bewusst,

Kontakt:
Landeskriminalamt Nordrhein-Westfalen
Völklinger Straße 49
40221 Düsseldorf

Stand: Februar 2021

dass der Mitschnitt einen Verstoß gegen die EU-DSGVO[2] darstellt.

> Kinder und Jugendliche nutzen im Homeschooling oftmals zum ersten Mal webbasierte Messengerdienste für Videokonferenzen, aber auch zur Absprache von Terminen. Dieses Medium steht ihnen fortan aber auch in Pausen oder nach dem Unterricht zur Verfügung und kann unkontrolliert genutzt werden.

> Manche Anwendungen verfügen über ein automatisch integriertes Adressbuch, welches anderen Personen ermöglicht, eine direkte Kontaktaufnahme zu starten.

> Informieren Sie sich über die genutzte Anwendung und sperren Sie bei der Konfiguration den Zugriff externer Personen aus.

> Klären Sie alle Nutzerinnen und Nutzer über bestehende Gefahren auf

Weiterführende Informationen

https://polizei.nrw/artikel/cyber-grooming

Förderung der Medenkompetenz von Kindern
https://www.polizei-beratung.de/startseite-und-aktionen/aktuelles/detailansicht/fit-fuers-internet-teil-1-medienkompetenz-von-kindern-foerdern/

Digitaler Unterricht - Tipps für Lehrende:
https://www.polizei-beratung.de/startseite-und-aktionen/aktuelles/detailansicht/fit-fuers-internet-teil-2-tipps-fuer-lehrende/

[2] EU_Datenschutzgrundverordnung

Kontakt:
Landeskriminalamt Nordrhein-Westfalen
Völklinger Straße 49
40221 Düsseldorf

Stand: Februar 2021