

Verhaltensempfehlungen für die Beratung der Schulen im Umgang mit dem Phänomen "Gehackter Distanzunterricht"

Organisatorische Maßnahmen

- Um im Klassenverband zeitnah auf entsprechende Vorfälle reagieren zu können, wird empfohlen, einen einheitlichen E-Mail Verteiler der jeweiligen Klasse durch die Klassenlehrer einzurichten und diesen stets aktuell zu halten.
- Es wird empfohlen, für den Onlineunterricht einen geschlossenen Teilnehmerkreis zu nutzen und die Pseudonyme der Schülerinnen und Schüler so festzulegen, dass eine eindeutige Identifikation des jeweiligen Gruppenmitglieds möglich ist.
Unberechtigte können so schnell identifiziert und aus dem Meeting entfernt werden.
Um eine Verwendung von Klarnamen der Schülerinnen und Schüler zu vermeiden, kann hierbei beispielsweise auf eine der nachfolgenden Kombinationen zurückgegriffen werden:
 - Vorname und Klasse
 - Vorname und erster Buchstabe des NachnamensSofern vollständig auf Namensbestandteile verzichtet werden soll, wird empfohlen, den jeweiligen Schülerinnen und Schülern entsprechende Pseudonyme (z. B. Schüler*in 1-20, Kind 1-20 etc.) durch die Lehrkraft zuzuweisen.
- Vor der erstmaligen Nutzung eines neuen Videokonferenzsystems sollte sich die Lehrkraft mit allen Funktionen ausgiebig vertraut machen und Gelegenheit erhalten, diese Nutzung zu üben. Nicht benötigte Funktionen sollten abgeschaltet werden.

Technische Maßnahmen

- Es sollten von den Lehrkräften nur Programme mit Moderatorensperre verwendet werden. Hierbei entscheidet der Moderator, ob ein Person Zutritt zur Online-Konferenz erhält oder nicht.
- Sofern möglich, sollte eine Online-Schaltkonferenz nach Beginn gesperrt werden, wodurch weitere Personen am Betreten des Onlineunterrichtes gehindert werden.
- Sofern möglich, sollten Videokonferenzsysteme mit Passwortschutz verwendet werden. Hierbei ist darauf zu achten, dass der Einladungslink getrennt vom Passwort übermittelt wird.
Einladungslinks dürfen niemals öffentlich verbreitet oder weitergeben werden.
- Private Chatmöglichkeiten sollten durch den Moderator deaktiviert werden.
- Die Bildschirmfreigabe sollte grundsätzlich deaktiviert sein und nur durch die Lehrkraft freigegeben werden können.

Sicherung der mobilen Endgeräte

- Es sollte sichergestellt werden, dass die zur Einwahl in den Onlineunterricht verwendeten mobilen Endgeräte vor einem unberechtigten Zugriff geschützt sind.
Die Geräte sollten über einen PIN- oder Passwortschutz sowie über eine Bildschirmsperre mit kurzer Aktivierungszeit verfügen.
Bei einer Abwesenheit sollten die Teilnehmenden dahingehend sensibilisiert werden, dass Sie die ihre mobilen Geräte sperren.

Weitergehende Hinweise zur Sicherung von mobilen Endgeräten gibt es unter www.polizei-beratung.de oder auf www.polizei.hessen.de.

Im Ereignisfall

Sofern es trotz der vorgenannten Maßnahmen zu einem Zwischenfall kommen sollte, wird folgendes Vorgehen empfohlen:

- Entfernen Sie grundsätzlich nicht eingeladene Personen aus dem Meeting.
- Sofern es sich um strafrechtlich relevante Sachverhalte handelt, sollten umgehend Screenshots zur Beweissicherung angefertigt werden und Anzeige bei der zuständigen Polizeidienststelle erstattet werden.
- Beenden Sie bei Zwischenfällen mit Schülerinnen und Schülern die Sitzung umgehend und stellen Sie neue Zugangsdaten mit einem neuen Passwort zur Verfügung.

Ansprechpersonen

Im Bereich der kriminalpolizeilichen Prävention stehen in jedem Polizeipräsidium Ansprechpersonen für die Bereiche Jugendkoordination, Prävention Cybercrime und Opferschutz für entsprechende Beratungen zur Verfügung.

Die Übersicht aller Ansprechpartner ist auf www.polizei.hessen.de eingestellt.

Für Rückfragen stehen Ihnen alle LandeskoordinatorInnen der Prävention im HLKA gerne zur Verfügung.

Mit den besten Grüßen aus Wiesbaden
Im Auftrag

Thomas Lorenz

Leitung Zentralstelle für Kriminal- und Verkehrsprävention



Hessisches Landeskriminalamt
Hölderlinstraße 1 - 5
65187 Wiesbaden
Tel.: 0611 / 83 -13000
Gz: 0611 / 83 - 13009
E-Mail: hsg13-l@polizei.hessen.de