Verbraucherschützer warnen vor LGBTQ+ Extortion Scams

Romantik- und Porno-Scams werden vermehrt in Kombination und aggressiv eingesetzt. Besonders auf noch nicht geoutete Personen der LGBTQ+ Gemeinschaft haben die Kriminellen ein Auge geworfen.

Seit geraumer Zeit wird vor Romance-Scammern und Porn-Scammern gewarnt. Jetzt versuchen es die Cyberkriminellen mit einer hybriden Kombination aus beidem und haben dabei auch die LGBTQ+ Gemeinde im Visier. Die US-amerikanische Verbraucherschutzbehörde Federal Trade Commission (FTC) hat daher eine besondere Warnung vor dieser Art von Erpressung für Menschen aus der LGBTQ+-Gemeinschaft herausgegeben, die sich noch nicht „geoutet" haben.

Die Masche
Mit der hybriden Kombination aus Romantik-Porno-Scam sprechen die Cyberkriminellen ihre Opfer in der Regel auf einer Dating-Website an. Dies entspricht im ersten Schritt der klassischen Vorgehensweise, bei der die Romantic-Scammer, um das Interesse und Vertrauen ihrer Opfer werben. Der Unterschied mit der hybriden Masche liegt jedoch darin, dass sich die Scammer kaum Zeit nehmen, die Opfer über einen längeren Zeitraum um Geld zu bitten. Stattdessen überreden sie sie dazu, explizite Fotos auszutauschen. Die Betrüger täuschen Vertrauen vor, indem sie selbst angebliche eindeutige Fotos senden – wie man sich vorstellen kann, sind diese natürlich nicht von den Scammern. Anschließend wechseln die Betrüger in den Porn-Scam-Modus und versuchen Schweigegeld zu erpressen: „Zahlen Sie Schweigegeld, oder wir werden die Informationen und Fotos an Leute weitergeben, die nichts davon wissen sollen". Der Unterschied zum klassischen Porn-Scam, der in nahezu allen Fällen ein Fake ist, liegt darin, dass die Scammer jetzt tatsächlich über prekäres Material ihrer Opfer verfügen.

Als wenn sexuelle Erpressung noch nicht schlimm genug ist, haben es die Betrüger nun auch auf Opfer abgesehen, deren Sexualität ein Geheimnis ist – darunter zurückhaltende oder noch nicht geoutete Menschen aus der LGBTQ+-Gemeinschaft.

Die FTC erklärt:
Die Kriminellen gehen in der Regel folgendermaßen vor: Ein Betrüger gibt sich auf einer LGBTQ+-Dating-App als potenzieller Liebespartner aus, chattet mit seinem Opfer, schickt schnell explizite Fotos und verlangt im Gegenzug ähnliche Bildaufnahmen. Wenn die Opfer Fotos schicken, beginnt die Erpressung. Die Betrüger drohen damit, die Gespräche und Fotos an Freunde, Familie oder Arbeitgeber weiterzugeben, wenn das Opfer nicht bezahlt …..

Empfehlungen von Sophos

- **Umgekehrte Bildsuche:** Mit einer umgekehrten Bildsuche im bevorzugten Browser lassen sich zwar selten die Betrüger aufspüren, aber es kann helfen zu erkennen, dass jemand, den man gerade auf einer Dating-Website „kennengelernt" hat, nicht die Person ist, für die sie sich ausgibt. Mit anderen Worten: Wenn die umgekehrte Bildsuche keine nützlichen Treffer liefert, beweist das nicht, dass die Person echt ist. Wenn man jedoch einen Treffer für das Profil einer anderen Person erhält, kann man sicher sein, dass es sich um einen Betrüger handelt.

- **Restriktives Teilen persönlicher Daten und Informationen:** In vielen Ländern ist es nicht illegal, explizite Fotos an andere Personen zu senden, wenn beide Parteien damit einverstanden sind. Dies setzt jedoch nicht nur voraus, dass man der anderen Person

vollkommen vertraut, sondern auch, dass man nicht selbst Opfer eines Hacks oder einer Datenschutzverletzung wird, bei der die weitergegebenen Informationen von jemand anderem abgegriffen und weiterverkauft werden.

- **Privates bleibt privat:** Im Zweifelsfall gilt es nichts weiterzugeben, was nicht öffentlich bekannt werden soll. Man sollte Personen, die man nicht wirklich kennt und die man noch nie getroffen hat, nichts anvertrauen. Informationen, die einmal preisgegeben sind, können nicht zurückgerufen werden – egal wie kooperativ die Personen, denen man sie anvertraut hat, auch erscheinen mögen.

- **Keinesfalls bezahlen:** Erpressungsforderungen sollten keinesfalls bezahlt werden. Es gibt keine Sicherheit, dass die Kriminellen die Daten wirklich löschen, auch wenn sie es behaupten oder versprechen. Schlimmer noch: Selbst, wenn die Betrüger die Daten tatsächlich löschen, gibt es keine Garantie, dass sie die Daten zuvor nicht weiterverkauft haben oder dass sie nicht selbst von anderen Gaunern gehackt wurden.

Social Media von Sophos für die Presse
Wir haben speziell für Sie als Journalist*in unsere Social-Media-Kanäle angepasst und aufgebaut. Hier tauschen wir uns gerne mit Ihnen aus. Wir bieten Ihnen Statements, Beiträge und Meinungen zu aktuellen Themen und natürlich den direkten Kontakt zu den Sophos Security-Spezialisten.
Folgen Sie uns auf und

LinkedIn: https://www.linkedin.com/groups/9054356/
Twitter: @sophos_info

Pressekontakt:

Sophos
Jörg Schindler, PR-Manager Central & Eastern Europe
joerg.schindler@sophos.com, +49-721-25516-263

TC Communications
Arno Lücht, +49-8081-954619
Thilo Christ, +49-8081-954617
Ulrike Masztalerz, +49-30-55248198
Ariane Wendt +49-172-4536839
sophos@tc-communications.de