17. Oktober 2018, 10.00 Uhr MESZ

PRESSEMITTEILUNG

Klicken Sie hier und sehen Sie, wie Ihr Geld verschwindet – kriminelle #CyberScams des 21. Jahrhunderts

Europol und der Europäische Bankenverband starten Sensibilisierungskampagne zu den sieben häufigsten Online-Finanzbetrügereien

BRÜSSEL/DEN HAAG – Das Europäische Zentrum zur Bekämpfung der Cyberkriminalität (EC3) von Europol, **der Europäische Bankenverband** sowie deren Partner aus dem öffentlichen und privaten Sektor starten heute die Awarenesskampagne **#CyberScams** im Rahmen des European Cyber Security Month.

Im Laufe der nächsten Woche werden Strafverfolgungsbehörden aus allen **28 EU-Mitgliedstaaten, 5 Nicht-EU-Mitgliedstaaten[1], 24 nationalen Bankenverbänden** sowie Banken und viele andere Bekämpfer der Cyberkriminalität das Bewusstsein für dieses kriminelle Phänomen schärfen. Dieses gesamteuropäische Vorhaben wird durch eine Kommunikationskampagne über Social-Media-Kanäle sowie durch die nationalen Strafverfolgungsbehörden, Bankenverbände und Finanzinstitute vorangetrieben.

Gemäss den Empfehlungen der IOCTA 2018 besteht die effektivste Verteidigung gegen Social Engineering in der Sensibilisierung potenzieller Opfer, womit jeder und jede von uns gemeint ist, sobald wir online gehen. Die Sensibilisierung der Öffentlichkeit zur Identifizierung solcher Methoden zur Täuschung, helfen sowohl persönliche als auch finanzielle Daten bei Online-Aktivitäten zu schützen.

Für diese Kampagne wurde Awareness-Material **in 27 Sprachen** entwickelt, welches der Öffentlichkeit zum Download zur Verfügung gestellt wird. Das Material enthält Informationen über die sieben häufigsten Online-Finanzbetrügereien und Tipps wie man sie vermeiden kann:

- **CEO-Betrug**: Betrüger geben vor, Ihr CEO oder ein ranghoher Vertreter Ihrer Organisation zu sein und verleiten Sie dazu, eine gefälschte Rechnung zu bezahlen oder eine unbefugte Überweisung vom Geschäftskonto vorzunehmen.
- **Rechnungsbetrug**: Betrüger geben vor, einer Ihrer Kunden/Lieferanten zu sein und verleiten Sie dazu, zukünftige Rechnungen auf ein anderes Bankkonto zu bezahlen.
- **Phishing / Smishing/ Vishing**: Die Betrüger rufen Sie an oder senden Ihnen eine SMS oder eine E-Mail, um Sie dazu zu verleiten, Ihre

[1] Kolumbien, Liechtenstein, Norwegen, die Schweiz und die Ukraine

persönlichen, finanziellen oder sicherheitsrelevanten Informationen preiszugeben.

- **Gefälschte Bankwebsite**: Die Betrüger verwenden Phishing-E-Mails, die vorgeben, von einer echten Bank zu sein. Diese enthalten einen Link zu einer gefälschten Website. Sobald Sie auf den Link klicken, werden verschiedene Methoden zur Erfassung Ihrer finanziellen und persönlichen Daten verwendet. Die Website sieht, mit kleinen Unterschieden, wie die Website der echten Bank aus.
- **Romantik Betrug**: Die Betrüger täuschen vor, an einer romantischen Beziehung interessiert zu sein. Dies geschieht häufig auf Online-Dating-Websites. Betrüger benutzen aber auch oft Social Media oder E-Mails, um Kontakt aufzunehmen.
- **Datendiebstahl**: Die Betrüger schöpfen Ihre persönlichen Daten über Social-Media-Kanäle ab.
- **Anlage- und Online-Shopping-Betrug**: Die Betrüger täuschen vor, eine aussichtsreiche Investition anzubieten... oder sie präsentieren Ihnen ein grossartiges gefälschtes Online-Angebot.

Das Internet ist für Cyberkriminelle sehr attraktiv geworden. Angreifer verwenden raffinierte Tricks und Versprechungen, um Geld oder wertvolle Finanzinformationen aus Ihnen herauszuholen. Betrügereien mit Bezug zu einem längst verstorbenen Verwandten oder nigerianischen Prinzen sind nicht mehr die einzigen Tricks in der Schublade. Die Taktiken der Cyberkriminellen werden zunehmend innovativer und auch schwieriger zu erkennen. Vom Vortäuschen, CEO Ihrer Organisation zu sein, bis hin zum Vorgeben eines romantischen Interesses, unternehmen die Online-Betrüger von heute alles Mögliche, um das zu bekommen, was sie wollen – nämlich Ihr Geld und/oder Ihre Bankverbindung.

Wie in der Beurteilung der Bedrohungslage durch die organisierte Kriminalität im Internet (IOCTA) 2018 hervorgehoben, wächst Social Engineering weiter als Motor vieler Cyberverbrechen, wobei Phishing die häufigste Form ist. Kriminelle nutzen Social Engineering, um eine Reihe von Zielen zu erreichen: Ihre persönlichen Daten zu erhalten, Ihre Konten zu hacken, Ihre Identität zu stehlen, illegitime Zahlungen einzuleiten oder Sie zu überzeugen, eine beliebige andere Handlung gegen Ihr Eigeninteresse zu unternehmen, wie z.B. einen Geldtransfer oder die Weitergabe persönlicher Daten. Ein einziger Klick kann ausreichen, um Ihre gesamte Organisation zu gefährden.

Lesen Sie auf der speziellen Webseite von #CyberScams mehr darüber, wie Sie sich schützen können.

Der European Cyber Security Month (ECSM) ist eine EU-weite Awareness-Kampagne, die die Cybersicherheit bei Bürgern und Organisationen fördert und einfache Schritte zum Schutz ihrer persönlichen, finanziellen und beruflichen Daten aufzeigt.

Verfolgen Sie die **#CyberScams**-Kampagne:

Europol und EC3 Twitter, Facebook, Instagram, Youtube und LinkedIn
EBF Twitter, Facebook und Linkedin

LBV unterstützt europaweite Kampagne zur Sensibilisierung von Bürgerinnen und Bürger

Die stetige (Weiter-) Entwicklung von digitalen Geschäftsmodellen spielt im Bankensektor eine zentrale Rolle. Dabei steht im Vordergrund, dem Kunden attraktive und massgeschneiderte Dienstleistungen anbieten zu können. Die zunehmende Digitalisierung birgt jedoch das Risiko, Opfer von Cyber Attacken zu werden. Die liechtensteinischen Banken tätigen daher erhebliche Investitionen in die IT-Sicherheit, um dem Kunden den bestmöglichen Schutz vor Cyber Attacken bieten zu können.

Neben dem technischen Abwehrdispositiv ist jedoch die Bewusstseinsbildung des Nutzers von Online-Dienstleistungen von grundlegender Bedeutung. Der Liechtensteinische Bankenverband (LBV) und seine Mitgliedsbanken unterstützen daher vollumfänglich die gemeinsame Awareness Kampagne von Europol, dem Europäischen Bankenverband (EBF) und ihren Partnern aus dem öffentlichen und privaten Sektor. Neben der Sensibilisierung über Social-Media-Kanäle werden wir in der kommenden Woche durch verschiedene Artikel und Informationsmaterial auf einfache Weise die häufigsten Cyber Betrugs Attacken darstellen und erläutern, wie Sie Ihre persönlichen, finanziellen und beruflichen Daten im Rahmen von Online-Aktivitäten schützen können.