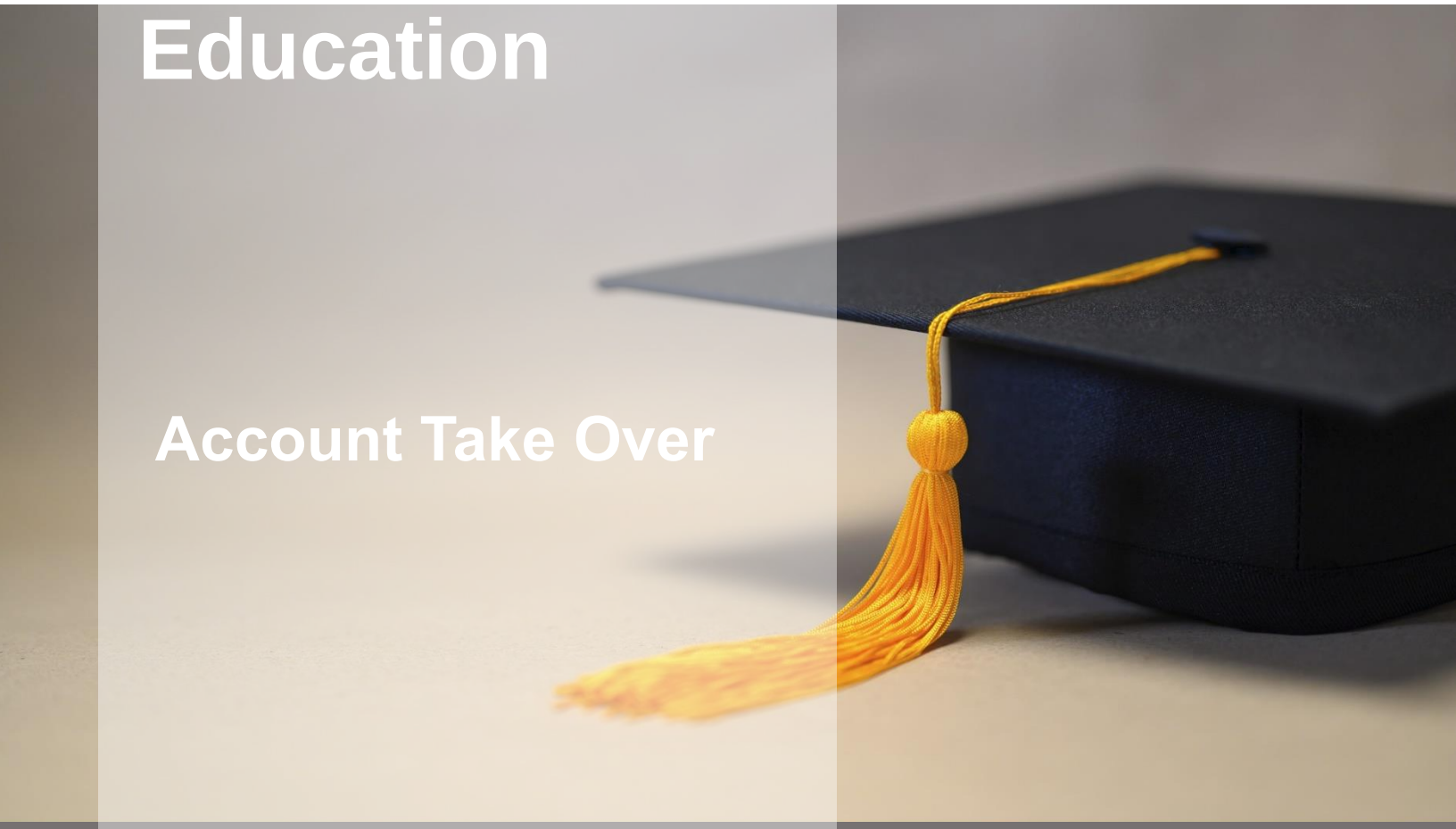
Consumer Education



Account Take Over

CONSUMER EDUCATION

Communications Fraud Control Association

Version 1.0

CFCA
Communications Fraud Control Association

Account Take Over

Providing insights, knowledge and learning when it comes to fraud.

DEFINITION:

ATO (Account Take over) -Fraudster obtains control over a consumer's existing online account, by hacking, phishing, etc., for PII data, or account harvesting, or to buy products/equipment (change of shipping address) or gain access to services/subscriptions.

MOTIVATION:

The primary motivation for account take over is financial gain. ATO attacks are most commonly used to steal payment credentials and other valuable information from the accounts. Fraudsters can apply for credit cards or loans using the information gained from ATO attacks. ATO attacks are also used to make fraudulent orders using stored credit card, steal loyalty points or reward points that can be used to purchase merchandise, gift cards, plane tickets etc. Fraudsters can also sell consumers credentials and accounts on the black market.

ADVICE TO CONSUMERS:

While there is no way to completely prevent account takeover as some factors are out of your control such as data breach leaks, there are some things that can be done to help protect your accounts.

* Use strong, complicated and unique passwords.
* Don't reuse passwords on multiple accounts.
* Update passwords every few months.
* Enable multi factor authentication when available.
* Monitor your identity, credit and bank accounts frequently for unusual activity

SOLUTIONS:

Communications fraud is the use of telecommunications products or services with no intention of payment. Fraud negatively impacts everyone, including residential and commercial customers. The losses increase the communications carriers' operating costs. Although communications operators have increased measures to minimize fraud and reduce their losses, criminals continue to abuse communications networks and services. Therefore, communications operators tend to keep their actual loss figures and their plans for corrective measures confidential. Due to the sensitive nature of this topic, CFCA used a confidential opinion survey of global communications operators to support the global fraud loss study.

About CFCA

CFCA is a not-for-profit global educational association that is working to combat communications fraud. The mission of the CFCA is to be the premier international association for revenue assurance, loss prevention and fraud control through education and information. By promoting a close association among telecommunications fraud security personnel, CFCA serves as a forum and clearinghouse of information pertaining to the fraudulent use of communications services. For more information, visit CFCA at www.CFCA.org.

Correspondence should be sent to fraud@cfca.org

Disclaimer of Liability

The material and information contained in this document is for general information purposes only. You should not rely upon the material or information in this document as a basis for making any business, legal or any other decisions.

Whilst we endeavor to provide correct information, CFCA makes no representations or warranties of any kind, express or implied about the completeness, accuracy, reliability, suitability or availability with respect to the information and graphics contained in this document for any purpose. Any reliance you place on such material is therefore strictly at your own risk.

CFCA will not be liable for any false, inaccurate, inappropriate or incomplete information presented in this document.

To the extent not prohibited by law, in no circumstances shall CFCA be liable to you or any other third parties for any loss or damage (including, without limitation, damage for loss of business or loss of profits) arising directly or indirectly from your use of information contained in this document.

www.cfca.org

Communications Fraud Control Association