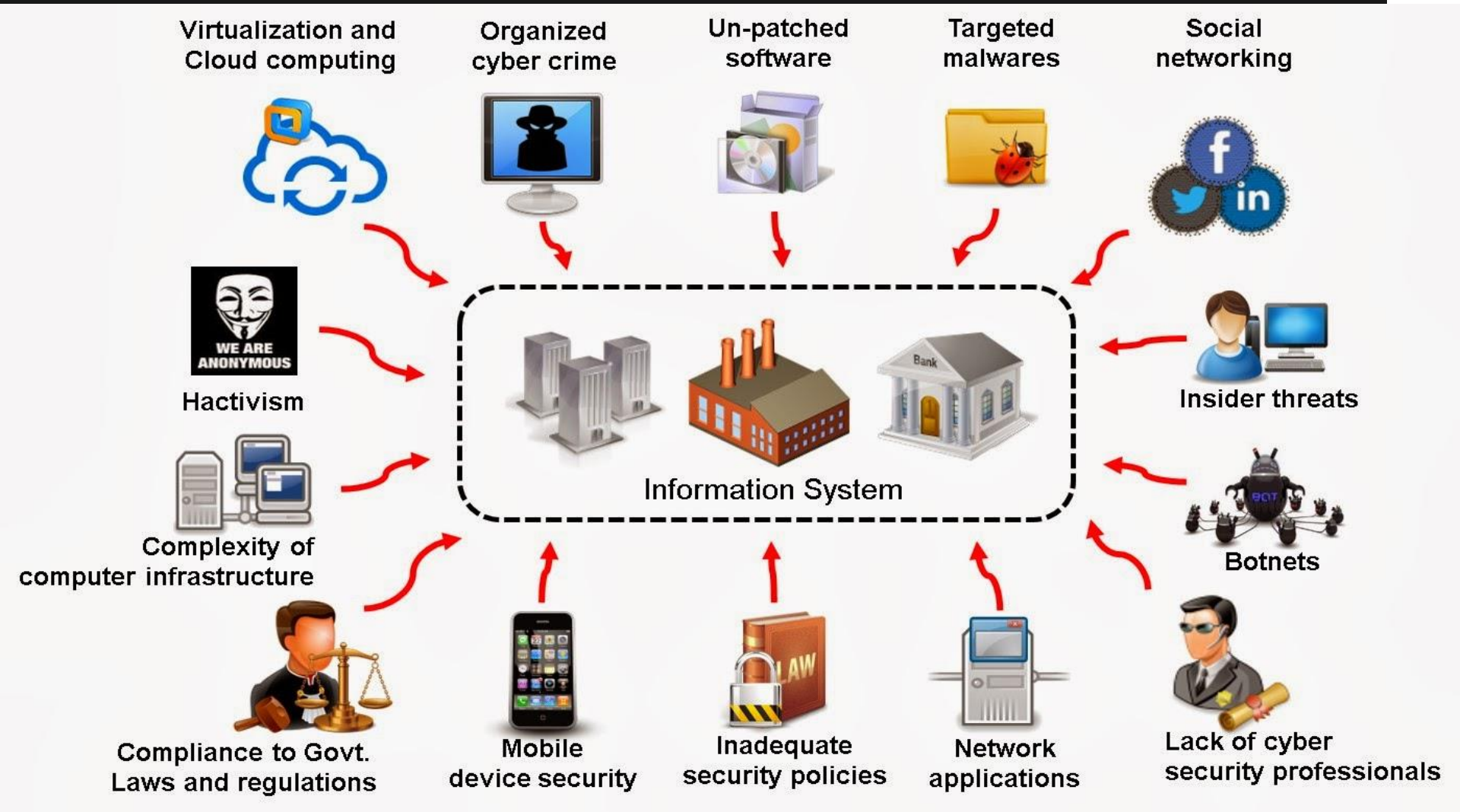
ცნობიერების ამაღლების მნიშვნელობა

ინფორმაციულ უსაფრთხოებაში

პრობლემა


Virtualization and Cloud computing
Organized cyber crime
Un-patched software
Targeted malwares
Social networking
WE ARE ANONYMOUS
Hactivism
Insider threats
Information System
Bank
Complexity of computer infrastructure
Botnets
Compliance to Govt. Laws and regulations
Mobile device security
Inadequate security policies
Network applications
Lack of cyber security professionals

Email?

რატომ Email?

- იაფი
  - Malware + Crypter + Mail List = ~500$
  - Phishing = 0$
- მასობრივი
  - ორგანიზაციების შეუზღუდავი რაოდენობა
- ეფექტური
  - შეტევა პირდაპირ საბოლოო წერტილზე, ანუ მომხმარებელზე.
  - ყველაზე სუსტი რგოლი დაცვის ჯაჭვში.

საფრთხეები Email-დან:

ცნობილი შეტევები:

- Anthem
- Sony Pictures
- Democratic Party (Fancy Bear)
- Wannacry და ა.შ.

მალსპამ კამპანიები:

- Emotet
- Lokibot
- ათობით Ransomware და ა.შ.

რეკლამა

რატომ არის TBC ერთ-ერთი ყველაზე დაცული ორგანიზაცია:

- ძვირადღირებული უსაფრთხოების გადაწყვეტილებები?
- კარგი კადრები უსაფრთხოებაში?:D
- ყველა პროექტში ინფორმაციული უსაფრთხოების ჩართულობა?

რეკლამა

რატომ არის TBC ერთ-ერთი ყველაზე დაცული ორგანიზაცია:

- გააჩნია თანამშრომელთა ტრეინინგის რამდენიმე ეტაპიანი სისტემა:
  - ერთჯერადი ფიზიკური ტრეინინგი
  - ონლაინ ტრეინინგი + ტესტირება წელიწადში რამდენჯერმე
  - **ფიშინგ სიმულაცია**

ონლაინ ტრეინინგი

რატომ ონლაინ ტრეინინგი?

- იაფი
  - Open Source გადაწყვეტილებები
  - ერთი პატარა ვებ სერვერი
  - ტრეინინგის ერთჯერადი შედგენა

- ეფექტური (არც მთლად..)
  - თანამშრომელი საქმის კურსშია შესაძლო საფრთხეების შესახებ

ფიშინგ სიმულაცია

რატომ ფიშინგ სიმულაცია?

- იაფი
  - Open Source გადაწყვეტილებები
  - ერთი პატარა ვებ სერვერი
- ეფექტური (ძალიან..)
  - თანამშრომელი დაშინებულია :)

ფიშინგ სიმულაცია

როგორ მუშაობს?

- იქმნება ფიშინგ გვერდი
- იქმნება საგანმანათლებლო (ანუ დასაშინებელი) გვერდი
- ეგზავნება ორგანიზაციის თანამშრომლებს

ფიშინგ სიმულაცია

გამარჯობა ირაკლი

გაცნობებთ, რომ ბანკში დაინერგა [redacted], რომელსაც შეემატა უამრავი ახალი ფუნქცია. ახალი პორტალიდან შეგიძლიათ იხილოთ ისეთი ინფორმაციები, როგორიცაა ხელფასები და შესაძლო ბონუსები.

ახალ [redacted]პორტალზე შესვლა შეგიძლიათ მოახდინოთ ქვემოთ მოცემული ბმულიდან (ავტორიზაცია ხდება ისევ ძველი მომხმარებლის სახელით და პაროლით).

ახალ პორტალზე შესვლა შესაძლებელია მხოლოდ ბანკის შიდა ქსელიდან!

http[redacted]tbcbank.com.ge

პატივისცემით

ადამიანთა რესურსების მართვის განყოფილება

ფიშინგ სიმულაცია

შენ გახდი ფიშინგის მსხვერპლი!

აღნიშნული გვერდი და ელ. წერილი რომლიდანაც მოხვდით ამ გვერდზე, არის თიბისი ბანკის ინფორმაციული უსაფრთხოების განყოფილების, ცნობიერების ამაღლების პროექტის ნაწილი.

წერილი საიდანაც თქვენ ამ გვერდზე მოხვდით, წარმოადგენს ფიშინგ წერილის სიმულაციას. ფიშინგ წერილები გამოიყენება ბოროტმოქმედების მიერ, რათა მოხდეს ორგანიზაციის თანამშრომლებიდან ინფორმაციის მოტყუებით მოპოვება, კომპიუტერის დავირუსება და ა.შ. თქვენ მოხვდით ფიშინგ წერილის სიმულაციის პროექტში, რათა თქვენთვის მოგვეხდინა დემონსტრაცია იმისა, თუ როგორ მუშაობს ფიშინგის ტიპის თაღლითობები და რა ადვილი შეიძლება იყოს პიროვნების მოტყუება.

იმ შემთხვევაში, რომ ეს წერილი ნამდვილი ფიშინგ თაღლითობის ნაწილი ყოფილიყო, ბმულზე გადასვლისას თქვენ შესაძლოა დაგეინფიცირებინათ საკუთარი კომპიუტერი. ან თუ თქვენ მართლა ჩაწერდით თქვენი მომხმარებლის სახელს და პაროლს ყალბ ვებ გვერდზე, ეს ინფორმაცია აღმოჩნდებოდა თაღლითების კონტროლ ქვეშ.

სურათზე ნაჩვენებია ის იდენტიფიკატორები, რისი მეშვეობითაც შეგიძლიათ შეამჩნიოთ გაყალბებული წერილი. მაგალითად გამომგზავნის ელ.ფოსტის მისამართი არის გაურკვეველი mail@tbcbank.com.qe (ბოლოს .QE და არა .GE) დომეინიდან. მეორე იდენტიფიკატორი კი არის ბმულის რეალური დანიშნულების მისამართი, რომელიც ჩანს ბმულთან კურსორის მიტანისას.

ასევე ტექსტი დაშვებულია გრამატიკული შეცდომები, რაც ასეთ შემთხვევებში მიუთითებს ხოლმე, რომ ის შეიძლება ავტომატური სერვისების მიერ იყოს გადმოთარგმნილი უცხო ენიდან.

გთხოვთ, რომ მომავალში იყოთ უფრო ფრთხილი და დაკვირვებული უცხო ბმულების გახსნისას!

მე ვაცნობიერებ თუ რა საფრთხეს შეიცავს ფიშინგ შეტევა და მომავალში ყოველთვის დავაკვირდები შემოსულ წერილებს.

გთხოვთ მონიშნოთ უჯრა და დააჭიროთ ღილაკს "I agree" ☐ I agree

ფიშინგ სიმულაცია

შედეგი:

- თანამშრომელი საქმის კურსშია არამარტო საფრთხეების, არამედ მათი მუშაობის პრინციპების შესახებ
- თანამშრომელს გაცნობიერებული აქვს საფრთხე, რაც მისმა ერთმა კლიკმა შეიძლება გამოიწვიოს
- ორგანიზაციას იცავს არა მარტო 1-2 ადამიანი, არამედ ყველა თანამშრომელი.

ფიშინგ სიმულაცია

ცნობილი გადაწყვეტილებები:

- Gophish - https://github.com/gophish/gophish
- Swordphish - https://github.com/certsocietegenerale/swordphish-awareness
- InstaPhishing (Beta) - https://www.rapid7.com/products/insightphishing/
- Simple Phishing Tookit - x_x

მადლობა