Phishing



Common methods used by attackers

- Pretending to be someone else
- Prey on your curiosity
- Using a fake sign in page
- Offering something too good to be true

From: domain@domain-name.com

To: Your email

Subject: Apple Facetime Information Disclosure



National Security Department

A vulnerability has been identified in the Apple Facetime mobile applications that allow an attacker to record calls and videos from your mobile device without your knowledge.

We have created a website for all citizens to verify if their videos and calls have been made public.

To perform the verification, please use the following link:

Facetime Verification

This website will be available for 72 hours.

National Security Department

Common signs of phishing

- Altered website links
- Fake emails
- Poor spelling or grammar

Reminder: [Recent News] [Statement Appointment] Information Updates - New Notice: We sent Summary of your bill has expire, Renews your membership Sunday, Jan 22, 2020 [Statement:- [FWD] Case ID: M68EXXSC TeamNetflix <noreplyrthismailerid33@ieuwgfiuwegfi NETFLIX Automatic payment. Hi Customer. Your Auto payment cannot process. Your subscription period will end on Wed, January 22, 2020. Click Here to update payment method please update your payment methode for continue Netflix feature. The Netflix Team

What to do if you see a phishing message

- Don't open the message, contact the sender through a different medium.
- If you think something is fake treat it as such
- Tell people so others know about the phishing campaign

What to do if you think you have been phished

- Change any username and passwords that the attacker may have stolen
- If they took your credit card information contact your bank
- Make sure all information that was stolen is rendered useless

