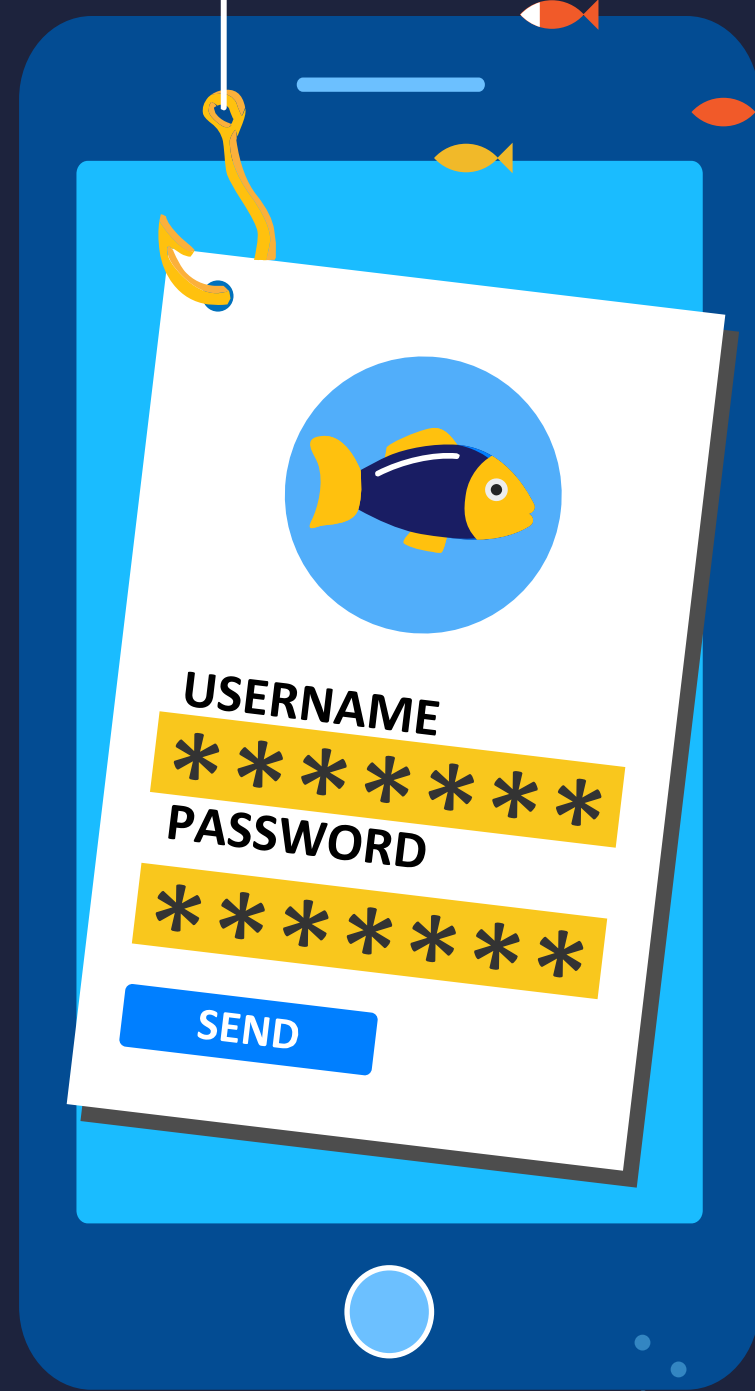




SI TË MBRONI TELEFONIN TUAJ.

MENDOHUNI DY HERË PARA SE TË KLIKONI

Mund të humbisni të ardhurat tuaja, informacionet personale madje edhe të dhënat tuaja të ruajtura, nëse pajisja ndalon së funksionuari. Mos u mashtroni!



SI MUND TË NDODHË?



SULMET PHISHING: Sulmuesit manipulojnë përdoruesit për të dorëzuar të dhënat duke u paraqitur si një burim i besueshëm. Phishing përhapet përmes emaileve, mesazheve me tekst ose platformave të mediave sociale



SHFLETIMI I FAQEVE TË INTERNETIT: Pajisja celulare mund të infektohet thjesht duke vizituar një faqe interneti të pasigurt



SHKARKIMI I FILEVE: Emaillet mund të përmbajnë bashkëngjitje dhe linqe keqdashëse

PSE ËSHTË EFEKTIVE?

Pajisjet celulare **JANË TË LIDHURA** vazhdimisht me internetin



Faqet e internetit ne pajisjet celulare shfaqin URL-të në hapësirën e kufizuar të ekranit, duke e bërë të vështirë të shihet nëse domeni është i ligjshëm

CFARË MUND TË BËNI?



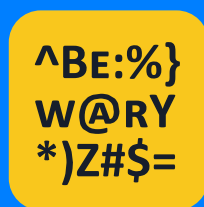
Tregohuni dyshues nëse merni një SMS ose një telefonatë nga një kompani që kërkon informacione personale. Ju mund të verifikoni që mesazhi apo telefonata është legjitime duke telefonuar drejtpërdrejt kompaninë në numrin e saj zyrtar.



Asnjëherë mos klikoni në një link ose bashkëngjitje në një email ose SMS të dyshimtë. Fshijeni menjëherë.



Kur shfletoni faqe interneti në pajisjen tuaj celulare, sigurohuni që lidhja juaj të jetë e siguar përmes HTTPS. Mund ta kontrolloni gjithmonë në fillim të URL-së.



Tregoni kujdes nëse hapni një website që përmban gramatikë të dobët dhe gabime drejtshkrimore.



Instaloni një aplikacion sigurie në telefon i cili do t'ju njoftojë për çdo aktivitet të dyshimtë.

