PHISHING

Ju merrni një email që duket sikur është nga dikush që njihni.

Duket sikur emaili vjen nga kompania ku punoni dhe kërkon që të klikoni në një link për të përditësuar llogarinë tuaj . A duhet të klikoni? A duhet të përgjigjeni?

SI

Funksionon phishing?

Ju mund të merrni një email ose mesazh

Duket se është nga dikush që njihni dhe ju kërkon të klikoni një link ose të jepni fjalëkalimin, llogarinë bankare ose informacione të tjera të ndjeshme.

Duket e vërtetë

Mashtruesit përdorin emra të njohur kompanish ose pretendojnë të jenë dikush që njihni.

Eshtë urgjente

Mesazhi ju shtyn të veproni tani – ose diçka e keqe do të ndodhë.

Çfarë ndodh më pas?

Nëse klikoni në një link, mashtruesit mund të instalojnë ransomware ose programe të tjera që mund t'ju bllokojnë nga të dhënat tuaja dhe të përhapen në të gjithë rrjetin tuaj.

ÇFARË **mund** TË BËNI

Përpara se të klikoni në një link ose të ndani informacionet të ndjeshme:

Kontrolloje

Kërkoni faqen e internetit ose numrin e telefonit për kompaninë ose personin që qëndron pas tekstit ose emailit. Sigurohuni që po merrni kompaninë e vërtetë dhe nuk po shkarkoni malware ose të flisni me një mashtrues.

Flisni me dikë

Biseda me një koleg mund t'ju ndihmojë të kuptoni nëse kërkesa është e vërtetë apo një përpjekje për phishing.

Ky material është përshtatur nga publikimi i përbashkët i organizatave: Federal Trade Commission, National Institute of Standarts and Technology, U.S Small Business Administration dhe Department of Homeland Security

Këshilla për

phishing

SI TË MBROHENI NGA PHISHING

Kreyeni Back up

Bëjini back up rregullisht të dhënave tuaja dhe sigurohuni që ato kopje rezervë të mos jenë të lidhura me rrjetin.

Mbani të përditësuar sigurinë tuaj

Gjithmonë instaloni përditësimet më të fundit. Kjo përfshin aplikacionet, web browserin dhe sistemet operative. Zgjidhni opsionin që përditësimet të ndodhin automatikisht.

Lajmëroni stafin tuaj

Përditësoni punonjësit për rreziqet dhe vulnerabilitetet e reja. Krijoni një kulturë sigurie duke zbatuar një plan periodik të trajnimit të punonjësve

Përdorni autentifikimin e emailit

Përdorni teknologjinë e autentifikimit të emailit për të ndihmuar në parandalimin e emaileve phishing

ÇFARË DUHET TË BËNI NËSE BINI PRE E NJË SULMI PHISHING

Lajmëroni të tjerët

Flisni me kolegët tuaj . Sulmet e phishing shpesh u ndodhin më shumë se një personi në një kompani.

Kufizoni dëmin

Ndryshoni menjëherë çdo fjalëkalim të komprometuar dhe shkëputni nga rrjeti çdo kompjuter ose pajisje që është e infektuar me malware.

Ndiqni procedurat e kompanisë suaj

Kjo përfshin njoftimin e njerëzve të veçantë në organizatën tuaj ose kontraktorëve që ju ndihmojnë me IT.

Njoftoni klientët

Nëse të dhënat tuaja personale janë kompromet uar, sigurohuni që të njoftoni palët e prekura – ato mund të jenë në rrezik të vjedhjes së identitetit.

Ky material është përshtatur nga publikimi i përbashkët i organizatave: Federal Trade Commission, National Institute of Standarts and Technology, U.S Small Business Administration dhe Department of Homeland Security