Siguria Kibernetike për

Bizneset e vogla

KËSHILLA PËR SIGURINË KIBERNETIKE

Kriminelët kibernetikë synojnë kompani të të gjitha madhësive

Njohja e këshillave të sigurisë kibernetike dhe zbatimi i tyre në praktikë do t'ju ndihmojë të mbroni biznesin tuaj dhe të zvogëloni rrezikun e një sulmi kibernetik.

MBRONI

SKEDARËT & PAJISJET TUAJA

Përditësoni softuerin tuaj

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

Siguroni skedarët tuaj

Bëni kopje rezervë të skedarëve në një hard disk të jashtëm ose në platformat cloud.

Vendosni fjalëkalime

Përdorni fjalëkalime për të gjitha pajisjet tuaja: laptop, tablet dhe telefonat. Mos i lini këto pajisje pa mbikëqyrje në vende publike.

Enkriptoni pajisjet

Kriptoni pajisjet dhe mediat e tjera që përmbajnë informacione të ndjeshme personale. Kjo përfshin laptopët, tabletët, telefonat ,USB, platformat cloud.

Përdorni vërtetimin me shumë faktorë

Kërkoni vërtetim me shumë faktorë për të hyrë në zonat e rrjetit tuaj me informacione të ndjeshme. Kjo kërkon hapa shtesë përtej hyrjes me një fjalëkalim - si një kod i përkohshëm në një smartphone ose si një çelës që futet në një kompjuter.

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

Siguria Kibernetike për

Bizneset e vogla

MBRONI RRJETIN TUAJ WIRELESS

Siguroni routerin tuaj

Ndryshoni emrin dhe fjalëkalimin e paracaktuar, çaktivizoni menaxhimin remote dhe bëni log-out si administrator pasi të konfigurohet routeri.

Përdorni të paktën enkriptimin WPA2

Sigurohuni që routeri juaj të ofrojë enkriptim WPA2 ose WPA3. Enkriptimi mbron informacionin e dërguar përmes rrjetit tuaj në mënyrë që të mos mund të lexohet nga personat e paautorizuar.

BËJENI SMART SECURITY ORGANIZATËN TUAJ

Vendosni fjalëkalime të forta

Një fjalëkalim i fortë ka të paktën 12 karaktere, të cilat janë një kombinim i numrave, simboleve dhe shkronjave të vogla dhe të mëdha.

Mos i ripërdorni asnjëherë fjalëkalimet dhe mos i shpërndani ato në telefon, në mesazhe ose me email.

Trajnoni stafin

Krijoni një kulturë sigurie duke zbatuar një plan periodik të trajnimit të punonjësve.

Përditësoni punonjësit për rreziqe dhe dobësitë e reja.

Nëse punonjësit nuk i ndjekin trajnimet, konsideroni masa për kufizimin e aksesit të tyre në rrjet.

Hartoni një plan

Hartoni një plan për ruajtjen e të dhënave, drejtimin e biznesit dhe njoftimin e klientëve nëse ju ndodh një shkelje në të dhënat e organizatës.

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