Siguria në internet

Mundësitë në internet janë praktikisht të pafundme. Interneti mundëson akses të shpejtë në informacion, komunikim global dhe funksione të tjera të ndryshme. Sidoqoftë, ai mbart gjithashtu rreziqe si malware, spam dhe phishing. Për të garantuar sigurinë tuaj në internet, është thelbësore të jeni të vetëdijshëm për këto kërcënime dhe të dini se si të shmangni ato.

Krijimi i fjalëkalimeve të forta

Do t'ju duhet të **krijoni një fjalëkalim** për të bërë pothuajse gjithçka në ueb, nga kontrollimi i emailit tuaj deri tek bankat online. Dhe ndërsa është më e thjeshtë të përdorësh një fjalëkalim të shkurtër dhe të lehtë për t'u mbajtur mend, kjo gjithashtu mund të përbëjë **rreziqe serioze** për sigurinë tuaj në internet. Për të mbrojtur veten dhe informacionin tuaj, do të dëshironi të përdorni fjalëkalime që janë **të gjata**, **të forta** dhe **të vështira për t'u marrë nga dikush tjetër,** ndërkohë që i mbani ato relativisht **të lehta për t'u mbajtur mend**.

Edhe pse shumica e faqeve të internetit janë të sigurta, ka gjithmonë një shans të vogël që dikush mund të përpiqet të hyjë ose të vjedhë informacionin tuaj. Kjo zakonisht njihet si **hakerim**. Një fjalëkalim i fortë është një nga mënyrat më të mira për të mbrojtur llogaritë tuaja dhe informacionin privat nga hakerët.

Udhëzime për krijimin e fjalëkalimeve të sigurta

Krijimi i një fjalëkalimi të sigurt përfshin krijimin e diçkaje të paharrueshme për ju, por sfiduese për të tjerët që ta hamendësojnë. Këtu janë disa këshilla thelbësore për t'u mbajtur parasysh:

- Shmangni përfshirjen e të dhënave personale si emri, ditëlindja, emri i përdoruesit ose emaili në fjalëkalimin tuaj, pasi këto shpesh mund të gjenden dhe hamendësohen lehtësisht.

- Këmbëngulni për fjalëkalime më të gjata. Synoni për një minimum prej gjashtë karakteresh, megjithëse më shumë karaktere do të thotë siguri e shtuar.
- Përdorni fjalëkalime unike për llogari të ndryshme për të parandaluar që një fjalëkalim i vetëm i kompromentuar të rrezikojë të gjitha llogaritë tuaja.
- Përfshini një përzierje të numrave, simboleve dhe shkronjave të mëdha dhe të vogla .
- Hiqni dorë nga fjalët e fjalorit, pasi ato mund të thyhen lehtësisht. Për shembull, 'shkolla1' është një zgjedhje e dobët.
- Fjalëkalimet më të sigurta janë të rastësishme. Nëse krijimi i një fjalëkalimi është sfidues, merrni parasysh përdorimin e një gjeneruesi të fjalëkalimeve për ndihmë.

Disa nga fjalëkalimet më të përdorura bazohen në **emrat e familjes** , **hobi** ose thjesht një **model të thjeshtë** . Ndërsa këto lloj fjalëkalimesh janë të lehta për t'u mbajtur mend, ato janë gjithashtu disa nga më pak të sigurtat.

Karakteristikat e sigurisë së shfletuesit tuaj

Kur shfletoni në internet, kompjuteri juaj është i ekspozuar ndaj kërcënimeve të ndryshme si viruset, malware dhe spyware. Për fat të mirë, shfletuesi juaj i internetit është i pajisur me karakteristika të shumta sigurie për të mbrojtur sistemin tuaj. Ne do të shqyrtojmë disa nga veçoritë kryesore që duhet të keni parasysh, së bashku me këshilla të thjeshta për t'u ndjekur për të rritur sigurinë tuaj në internet.

Kontrolloni adresën e internetit

Faqet e internetit me qëllim të keq shpesh përdorin adresa mashtruese të internetit për të mashtruar përdoruesit. Merrni, për shembull, një faqe interneti si **www.bankofarnerica.com** , e cila i ngjan shumë **www.bankofamerica.com** , por në mënyrë të hollësishme zëvendëson 'm' me ' rn '.

Për të verifikuar që po vizitoni një sajt legjitim, të besueshëm dhe jo një të rremë me një adresë të ngjashme, është e rëndësishme të kontrolloni me përpikëri emrin e domenit. Shumë shfletues të internetit ndihmojnë në këtë duke theksuar emrin e domenit me një ngjyrë më të errët brenda shiritit të adresave për ta bërë atë më të dukshëm. Për shembull, në shiritin e adresave, bankofamerica.com origjinale do të theksohej për të ndihmuar në dallimin e saj nga faqet mashtruese.

Shikoni simbolin e sigurisë

Disa faqe interneti do të shfaqin një **simbol bllokimi** në shiritin e adresave. Kjo më së shpeshti shihet me lloje të caktuara të faqeve të internetit, si dyqanet online dhe faqet bankare. Kjo do të thotë se faqja e internetit po përdor një lidhje **HTTPS** , e cila e bën të sigurt futjen e informacionit tuaj personal. Do të shihni gjithashtu **https** në fillim të URL-së.

Ju nuk do ta shihni këtë simbol në të gjitha faqet e internetit dhe kjo është në rregull - jo të gjitha faqet e internetit kanë nevojë për këtë shtresë shtesë sigurie. Megjithatë, duhet të shmangni futjen e çdo informacioni delikat, si p.sh. numrin e kartës suaj të kreditit, nëse nuk e shihni këtë simbol në shiritin e adresave.

Shmangia e spamit dhe phishing

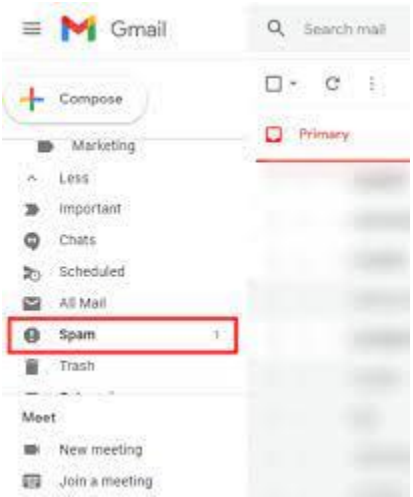
Interneti, duke përfshirë emailin, mesazhet e çastit dhe mediat sociale, është një mjet jetik për komunikim. Megjithatë, është gjithashtu një shesh lojërash i zakonshëm për mashtruesit dhe kriminelët kibernetikë. Për t'u mbrojtur kundër mashtrimeve me email, softuerëve të dëmshëm dhe vjedhjes së identitetit, është thelbësore të mësoni se si të dalloni dhe të shmangni përmbajtjen potencialisht të dëmshme në Inboxin tuaj, të tilla si spam dhe phishing.

Ballafaqimi me spam

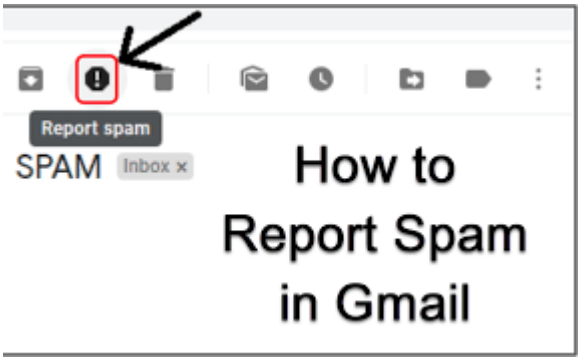
Spam-i, i njohur gjithashtu si email i padëshiruar, mbush Inboxin tuaj me reklama të padëshiruara dhe mund të fshehë rreziqe si phishing dhe malware. Shumica e shërbimeve të postës elektronike ofrojnë veçori për të ndihmuar në filtrimin e postës së padëshiruar, duke e mbajtur Inboxin tuaj më të sigurt.

Filtrat e spamit

Filtrat e postës së padëshiruar renditin mesazhet e padëshiruara në një dosje të padëshiruar për të parandaluar hapjen aksidentale. Megjithatë, këto sisteme nuk janë të pagabueshme dhe emailet e vërteta mund të filtrohen gjithashtu. Është e këshillueshme që të kontrolloni rregullisht dosjen tuaj të postës së padëshiruar për email të rëndësishëm të humbur:

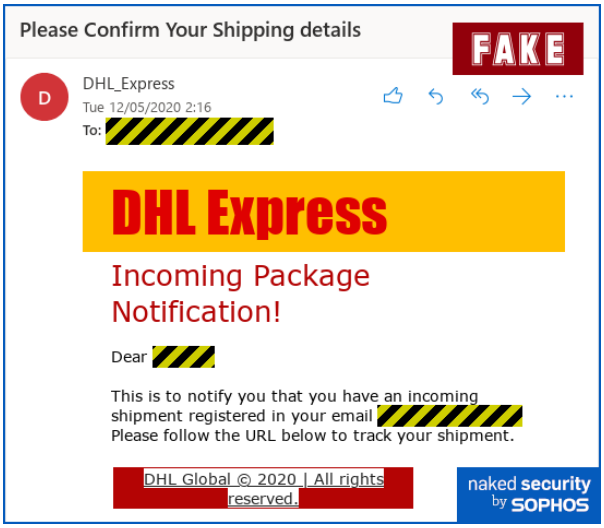


Shumë shërbime të postës elektronike kanë gjithashtu një veçori që mund ta përdorni për të shënuar emailet si të padëshiruara. Në Gmail, për shembull, mund të zgjidhni mesazhin dhe të klikoni butonin **Shënoni si të padëshiruar** . Kjo ndihmon ofruesin tuaj të emailit të filtrojë këto lloje mesazhesh në të ardhmen:



Phishing

Mashtrimet e phishing janë mesazhe mashtruese që synojnë marrjen e informacionit tuaj të ndjeshëm, si fjalëkalimet ose numrat e kartave të kreditit, shpesh duke u paraqitur si banka ose entitete të besuara. Ndërsa ato mund të duken autentike, mashtruesit krijojnë lehtësisht detaje bindëse. Ja se si një mashtrim përdor emrin e DHL për phishing:



Mashtrime të tjera të zakonshme me email

Spam dhe phishing janë të përhapura, por ekzistojnë edhe mashtrime të tjera me email. Disa ofrojnë shuma të mëdha parash në këmbim të një pagese paraprake, ndërsa të tjerë imitojnë kontaktet që njihni, duke kërkuar para ose duke ju nxitur të shkarkoni bashkëngjitjet.

Tregoni kujdes si me mesazhet e padëshiruara dhe phishing. Shmangni dërgimin e parave bazuar në një kërkesë me email dhe jini të kujdesshëm ndaj bashkëngjitjeve të papritura, pasi ato mund të përmbajnë malware që kërcënojnë kompjuterin tuaj dhe të dhënat personale.

Ndërsa evoluojnë taktikat e postës së padëshiruar, mashtrimet dhe phishing, të qenit i informuar se çfarë të shikoni dhe të shmangni ndihmon në mbrojtjen e Inboxit dhe kompjuterit tuaj.

Blerje të sigurta në internet

Blerja në internet është një mënyrë e përshtatshme për të blerë pothuajse çdo gjë nga komoditeti i shtëpisë tuaj. Dhe ndërsa ka disa rreziqe me blerjet në internet, ka gjithashtu shumë mënyra për të mbrojtur veten dhe informacionin tuaj financiar. Disa këshilla si më poshtë:

1. Blerja nga shtëpia - Për mbrojtje më të mirë të detajeve të ndjeshme si numrat e kartave të kreditit, këshillohet të bëni blerje duke përdorur lidhjen tuaj të internetit në shtëpi. Blerjet në Wi-Fi publik ose përdorimi i kompjuterëve publikë, rrit rrezikun e hakerimit dhe rrezikon potencialisht informacionin tuaj.
2. Siguria HTTPS - Kërkoni një simbol bllokimi në shiritin e adresave të faqes së internetit, zakonisht i dukshëm në faqen e pagesave të një dyqani online. Kjo tregon një lidhje HTTPS, duke siguruar të dhënat që futni. Ndërsa jo të gjitha faqet në një sajt blerjesh do ta kenë këtë simbol, shmangni futjen e informacionit financiar në faqet pa të.
3. Hulumtoni përpara se të blini - Është thelbësore të hulumtoni një kompani ose shitës në internet përpara blerjes. Verifikoni adresën e tyre fizike dhe numrin e kontaktit për çdo problem. Kontrolloni vlerësimet e

klientëve në platforma si Yelp dhe Google për të vlerësuar reputacionin e tyre.
4. Metodat e sigurta të pagesës - Kartat e kreditit janë shpesh mënyra më e sigurt e pagesës në internet. Është më mirë të shmangni transfertat direkte, transfertat bankare ose dërgimin e parave/çeqeve. Për siguri të shtuar, merrni parasysh përdorimin e shërbimeve të pagesave në internet si PayPal ose Google Wallet.
5. Mbani të dhënat e transaksioneve - Mbani të dhënat e transaksioneve në internet, duke përfshirë faturat, numrat e porosive, detajet e produktit dhe çmimet. Gjithashtu, mbani email nga shitësit, pasi ato mund të jenë të dobishme në rast mosmarrëveshjesh ose problemesh.

Siguria në internet për fëmijët

Për të garantuar sigurinë e fëmijëve tuaj në internet, është e rëndësishme të jeni të vetëdijshëm për rreziqet e ndryshme të internetit. Ata mund të hasin në përmbajtje të papërshtatshme, si pornografi ose gjuhë eksplicite. Për më tepër, ekziston rreziku i ngacmimit kibernetik ose ngacmimi në internet. Megjithëse nuk është e sigurt që fëmija juaj do të përballet me të gjitha këto kërcënime, të qenit i informuar për to mund t'ju udhëheqë ju dhe fëmijët tuaj në marrjen e zgjedhjeve më të sigurta në internet. Këtu janë disa udhëzime kryesore për edukimin e fëmijëve tuaj për të qëndruar të sigurt në internet:

1. Edukoni veten për internetin: Të kuptuarit e internetit ju ndihmon të kuptoni rreziqet dhe të komunikoni në mënyrë efektive me fëmijët tuaj rreth tyre.
2. Vendosni rregulla në internet: Vendosni kufij të qartë për atë që fëmijët tuaj mund dhe nuk mund të bëjnë në internet. Krijimi i udhëzimeve përpara se të lindë ndonjë problem është thelbësor.
3. Siguria e të dhënave personale: Instruktoni fëmijët tuaj për rreziqet e ndarjes së të dhënave personale si numrat e telefonit, adresat dhe informacionet e kartës së kreditit. Të dhëna të tilla mund të keqpërdoren nga kriminelët për të dëmtuar familjen tuaj.
4. Rrjetet e sigurta sociale: Mësojini fëmijët tuaj të përdorin mediat sociale me përgjegjësi. Kujtojuni atyre se çdo gjë e ndarë në internet, madje

edhe me miqtë, mund të përfundojë në duar të gabuara. Ata duhet të postojnë vetëm atë që ndihen rehat duke parë e gjithë bota.

5. Komunikimi i hapur: Inkurajoni fëmijët tuaj që t'ju drejtohen për çdo problem në internet. Është e rëndësishme të kuptojmë se ata mund të pengohen aksidentalisht në përmbajtje të papërshtatshme, madje edhe me qëllimet më të mira.
6. Diskutime të rregullta në internet: Bëni biseda të vazhdueshme me fëmijët tuaj rreth përdorimit të tyre të internetit. Diskutimet e shpeshta mund t'i bëjnë ata më të rehatshëm në qasjen ndaj jush për çdo problem që mund të hasin.

Urime, mësuat se si të përdorni internetin në mënyrë të sigurt!