UNIUNEA EUROPEANĂ

Instrumente Structurale 2014-2020

FiaTest
Mereu cu un pas înainte

GHID PRACTIC

privind securitatea informatică

DESPRE GHID

Într-o lume tot mai interconectată și digitalizată, securitatea informațiilor devine o prioritate atât pentru companii cât și pentru angajații acestora. Tehnologia ne oferă oportunități nesfârșite, dar, în același timp, ne expune și la riscuri de securitate cibernetică din ce în ce mai sofisticate.

Prezentul ghid a fost creat cu scopul de a te ajuta să navighezi într-un mod sigur, responsabil și conștient în era digitală. Aici, vei găsi o colecție de sfaturi practice și strategii concepute pentru a-ți proteja datele personale și pentru a contribui activ la securitatea informațiilor companiei la care ești angajat.

Ghidul este conceput pentru a fi accesibil și util tuturor angajaților, indiferent de cunoștințele acestora în domeniul securității cibernetice. Indiferent dacă ești începător în acest domeniu sau ai cunoștințe avansate, vei găsi informații valoroase care te vor ajuta să iei decizii informate și să acționezi în mod proactiv pentru a preveni amenințările cibernetice.

Prezentul ghid a fost elaborat de Fiatest în cadrul cursului de Formare de bază privind securitatea informatică desfășurat în cadrul proiectului „Educație și dezvoltare în era digitală" - proiect cofinanțat din Fondul Social European prin Programul Operațional Capital Uman 2014-2020. Contract de finanțare nr. POCU/860/3/12/143072

**Conținutul acestui material nu reprezintă în mod obligatoriu poziția oficială a Uniunii Europene sau a Guvernului României.*

FiaTest
Mereu cu un pas înainte

CREAREA PAROLELOR PUTERNICE

Infractorii cibernetici caută în permanență modalități de a trece de măsurile de securitate din cadrul companiei tale, una dintre cele mai ușoare modalități este ghicirea sau spargerea parolelor slabe, de aceea este importantă crearea parolelor puternice.

De obicei sistemele sau serviciile web au implementate propria politică de parole, ceea ce forțează utilizatorii să aleagă parole complexe, uneori chiar fiind constrânși să o schimbe la intervale predefinite. În cazul în care sistemul nu forțează utilizatorul să aleagă o parola complexă, sarcina de creare a unei parole puternice revine însuși utilizatorului.

Iată câteva recomandări pentru crearea unor parolele puternice și complexe:

Utilizează parole lungi

Cu cât o parolă are mai multe caractere, cu atât este mai dificil de spart. Este recomandat ca parola să conțină cel puțin 12 caractere.

Utilizează combinații complexe și unice

O parolă puternică trebuie să includă litere mici și mari, cifre și caractere speciale(de exemplu: @, #, $, %). Astfel, veți crea o parolă mai dificil de ghicit.

Parola nu tebuie să fie un cuvânt care poate fi găsit într-un dicționar sau numele unei persoane, caracter, produs sau organizație.

Nu reutiliza parolele

Fiecare cont trebui să aibă o parolă unică. În caz contrar, dacă o parolă este compromisă, toate conturile tale devin vulnerabile.

FiaTest
Mereu cu un pas înainte

PĂSTRAREA PAROLELOR ÎN SIGURANȚĂ

Păstrarea parolelor în siguranță este la fel de importantă precum crearea parolelor puternice. Iată câteva recomandări pentru a asigura că parolele tale rămân protejate:

Nu comunica nimănui parolele tale

Parola nu se comunică nimănui (nici prietenilor, membrilor de familiei, colegilor de muncă, superiorilor, personalului IT etc.). Parola trebuie păstrată în secret.

Evită notarea parolelor

Evită să scrii parolele pe hârtie, stickere sau să le stochezi în documente electronice necriptate, aceasta poate expune parolele la riscuri.
Pentru pastrarea parolelor este recomandată utilizarea unui manager de parole (Keepas, LastPass etc.)

Niciodată să nu expediezi parole prin text clar sau canale nesigure!

Evită introducerea parolelor pe dispozitive străine, care nu îți aparțin!

Utilizează autentificare în Doi Factori (2FA)

Activează autentificarea în doi factori oriunde este posibil. Această metodă adaugă un nivel suplimentar de securitate, necesitând un cod generat sau un SMS pe lângă parolă.

Schimbă regulat parolele

Chiar și o parolă puternică poate fi compromisă în timp. Pentru a-ți menține conturile în siguranță, schimbă-ți parolele în mod regulat.

Dacă crezi că există riscul ca parola să fie compromisă, schimb-o în cel mai scurt timp posibil.

FiaTest
Mereu cu un pas înainte

GESTIONAREA SIGURĂ A DISPOZITIVELOR

Calculatoarele/telefoanele mobile sunt valoroase pentru infractori nu doar pentru valoarea lor fizică, dar și pentru datele și informațiile pe care le conțin.
O pregătire și utilizare corectă a dispozitivelor ar putea diminua riscurile ca datele tale și a companiei să ajungă în mâinele infractorilor. În continuare sunt prezentate câteva recomandări pentru gestionarea sigură a dispoztivelor tale:

Setează o parolă de acces

Asigură-te că accesul la sistemul de operare al dispozitivului este restricționat cu o parolă sau cod PIN.

Actualizează regulat software-ul

Asigură-te că sistemul de operare și aplicațiile sunt actualizate la cele mai recente versiuni. Actualizările conțin adesea remedieri pentru vulnerabilități de securitate.

Instalează aplicații doar din surse de încredere

Descarcă și instalează aplicații numai din surse oficiale, cum ar fi pagina oficială a furnizorului de aplicație, Google Play Store sau App Store. Evită instalarea aplicațiilor din surse necunoscute.

Utilizează software de securitate

Instalează și utilizează software de securitate(firewall, antivirus) pentru a detecta și preveni amenințările cibernetice.

Realizează scanări periodice ale dispozitivului tău pentru a identifica prezența malware-ului, a aplicațiilor nedorite sau a altor amenințări cibernetice.

Efectuează regulat copii de siguranță (backup)

Pentru a preveni pierderea ireversibilă a datelor în cazul în care dispozitivul este deteriorat sau pierdut, efectuează cu regularitate copii de siguranță, fie în cloud, de exemplu în Google Drive, OneDrive, Dropbox etc. sau pe un hard disk extern.

FiaTest
Mereu cu un pas înainte

Criptează dispozitivul

Criptează datele stocate pe dispozitele tale sau tot sistemul de operare pentru a asigura că datele sunt protejate în cazul în care dispozitivul este pierdut sau furat.

Blochează ecranul

Configurează dispozitivul pentru a se bloca automat sau a se închide după un anumit interval de inactivitate.

Poți bloca imediat ecranul apăsând combinația de taste **WIN + L** pentru Windows sau **Control + Comandă + Q** pentru MacOS.

Nu permite colegilor de muncă, membrilor familiei sau altor persoane să acceseze dispozitivele de lucru.

Evita conectarea la rețele Wi-Fi publice

Evită să te conectezi la rețele Wi-Fi publice și nesigure, care pot fi expuse atacurilor de interceptare a datelor. Dacă trebuie să le folosești, utilizează o rețea virtuală privată (VPN).

Evită utilizarea stick-urilor USB

Stick-urile USB pot fi potențiale surse de amenințări cibernetice. Acestea pot fi infectate cu malware sau viruși care pot afecta dispozitivele pe care sunt conectate. Evită să utilizezi stick-uri USB, utilzează în schimb, FTP securizat, cloud etc.

Fii atent la securitatea fizică a dispozitivelor

Protejează dispozitivul de furt sau acces neautorizat. Nu-l lăsa nesupravegheat în locuri publice sau accesibile.

FiaTest
Mereu cu un pas înainte

E-MAILUL ȘI COMUNICAREA ONLINE

Securitatea e-mailului și a comunicării online este esențială pentru protejarea confidențialității și integrității datelor tale în mediul digital.
Iată câteva sfaturi pentru a asigura o comunicare online sigură:

Evită accesarea link-urilor și atașamentelor suspecte

Nu deschide link-uri sau atașamente din e-mail-uri suspecte sau de la surse necunoscute. Verifică veridicitatea link-ului trimis de expeditor. Acestea pot conține malware sau pot fi încercări de phishing.

Verifică extensia atașamentelor recepționate

Nu deschide fișiere cu extensii necunoscute. Configurează sistemul de operare să afișeze extensiile tuturor fișierelor

Verifică adresele de E-mail

Asigură-te că adresele de e-mail ale expeditorilor sunt autentice. Atacatorii pot folosi adrese false pentru a induce în eroare destinatarii.

Nu dezvălui informații personale sau confidențiale

Nu dezvălui informații personale sau confidențiale prin e-mail sau în mesaje online. În special, evită să oferi numere de cont bancar, parole sau alte date sensibile prin aceste canale.

Stabilește un canal alternativ de comunicare

Este recomandat să stabilești un canal alternativ de comunicare cu furnizorii sau clienții pentru a valida orice schimbare a practicilor comerciale stabilite. Această măsură adițională ajută la prevenirea unor eventuale atacuri de phishing sau compromiteri ale datelor.

Utilizează BCC în loc de CC

Protejează confidențialitatea adreselor de e-mail ale destinatarilor și evită expunerea involuntară a identității celorlalți destinatari utilizând BCC.

Evită utilizarea adreselor email de muncă în scopuri personale și invers.

FiaTest
Mereu cu un pas înainte

INCIDENTE DE SECURITATE CIBERNETICĂ

Incidentele de securitate cibernetică se referă la evenimentele sau acțiunile care afectează negativ securitatea și integritatea sistemelor informatice, datelor și rețelelor în mediul digital. Aceste incidente pot varia de la atacuri cibernetice sofisticate până la erori umane sau defecțiuni tehnice care conduc la expunerea, deteriorarea sau pierderea informațiilor sensibile sau critice.

Identificarea și raportarea corectă a unui incident de securitate cibernetică sunt etape critice pentru a proteja informațiile și a preveni eventualele consecințe grave.
Iată pașii pe care îi poți urma pentru a identifica și raporta un incident de securitate:

Identificarea Incidentului

Fii atent la orice activitate neobișnuită sau suspectă de pe orice dispozitiv sau resursă pe care o utilizezi, cum ar fi accese neautorizate, e-mailuri ciudate sau comportamente nefamiliare.

Fii atent la orice solicitare suspectă, în special cele financiare. Ar putea fi o înșelătorie!

Asigură-te că solicitările sau comunicările pe care le primești sunt autentice și nu reprezintă încercări de phishing sau atacuri cibernetice.

Dacă identifici un incident, izolează imediat sistemul sau rețeaua afectată, de exemplu prin blocarea accesului la internet, pentru a preveni răspândirea daunelor, însă nu încerca să-l gestionezi singur întrucât acesta ar putea duce la consecințe mai grave.

ÎN CAZUL UNUI INCIDENT DE SECURITATE, NU INTRA ÎN PANICĂ, CI RAPORTEAZĂ-L IMEDIAT.

Raportarea Incidentului

Raportează incidentul echipei de securitate a companiei tale. Dacă ești un utilizator individual, contactează furnizorul de servicii sau autoritățile în domeniul securității cibernetice.

Asigură-te că raportezi incidentul folosind canale sigure, pentru a preveni orice risc de expunere a informațiilor sensibile.

Notează toate detaliile relevante despre incident, inclusiv momentul în care l-ai descoperit, modul în care s-a produs și eventualele daune sau date afectate.

Oferă cât mai multe informații posibile cu privire la incident, inclusiv capturi de ecran, log-uri relevante sau alte detalii care pot ajuta în investigație.

Colaborează cu echipa de securitate urmând recomandările și instrucțiunile lor. Echipa de securitate va iniția o investigație și va lua măsurile necesare pentru a soluționa incidentul.

În anumite cazuri, poate fi necesar să notifici autoritățile competente, cum ar fi autoritățile de reglementare, Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal (ANSPDCP), Directoratul Național de Securitate Cibernetică (DNSC) etc.
Dacă incidentul afectează terțe părți, cum ar fi clienți sau parteneri de afaceri, informează-i cu privire la situație și măsurile luate pentru rezolvare.

Numărul unic de urgență la nivel național dedicat raportării incidentelor de securitate cibernetică este 1911 , apelabil din orice rețea, cu tarif normal, disponibil 24/7*.

Raportarea rapidă și eficientă a incidentelor de securitate cibernetică poate minimiza daunele și contribui la protejarea informațiilor și resurselor.

O comunicare transparentă și cooperarea cu profesioniștii în securitate cibernetică sunt esențiale pentru a aborda eficient astfel de situații.

FiaTest
Mereu cu un pas înainte

UNIUNEA EUROPEANĂ

Instrumente Structurale 2014-2020

DESPRE PROIECT

„EDUCAȚIE ȘI DEZVOLTARE ÎN ERA DIGITALĂ”

FiaTest împreună cu **Camera de Comerț și Industrie Iași** și **Asociația Iconic Cluster** implementează proiectul ”Educație și dezvoltare în era digitală”, proiect co-finanțat din Programul Operațional Capital Uman 2014 – 2020. Contract de finanțare nr. POCU/860/3/12/143072

Obiectivul general al proiectului constă în îmbunătățirea nivelului de competențe digitale în cadrul sectoarelor economice / domeniilor identificate conform Strategiei Naționale pentru Competitivitate și în corelare cu unul din domeniile de specializare inteligentă conform Strategiei Naționale de Cercetare, Dezvoltare și Inovare, prin îmbunătățirea nivelului de cunoștințe al angajaților din IMM-uri care activează în aceste domenii, în regiunile mai puțin dezvoltate, în special Regiunea Nord-Est.

Proiectul se desfășoară pe parcursul a 18 luni, 15 martie 2022 – 14 septembrie 2023.

/educatiesidezvoltareineradigitala

FiaTest și-a început activitatea în 1990, fiind prima companie românească de consultanță specializată în managementul calității și în educația adulților.

În 30 de ani de activitate, am sprijinit peste 400 de organizații, ne-am implicat în peste 60 de proiecte cu finanțare națională, europeană și internațională și am organizat cursuri deschise și personalizate, la care au participat peste 10.000 de cursanți.

Toate proiectele pe care le-am desfășurat s-au bazat pe experiența practică a echipei noastre și ne propunem, să oferim, în continuare, o gamă de servicii complexe și utile care să aducă organizațiilor performanțe sustenabile.

www.fiatest.ro

office@fiatest.ro

Str. Actor Ion Brezoianu nr.23-25, Corp A, Etaj 3,Sector 1, București

(+40) 758 11 33 07

/fiatestconsultantasiinstruire

/company/fiatest

FiaTest
Mereu cu un pas înainte