Securitatea online

Pe măsură ce vă propuneți să faceți afaceri pe web, veți întâlni trei tipuri specifice de oameni:

• Cei care vor să cumpere de la tine

• Cei care vor să fure de la tine

• Cei care vor să fure de la cei care cumpără de la tine

Paradoxul cu care se confruntă fiecare proprietar de site este că doriți să întâmpinați primul tip de persoană cu brațele deschise, dar pe ceilalți veți dori să încercați să le excludeți. Într-un magazin offline tradițional, este de obicei ușor de perceput de unde vor veni problemele. A face afaceri online înseamnă, totuși, că pierdeți orice intuiție importantă.

Securitatea trebuie să fie întotdeauna cea mai mare prioritate a dvs. dacă vindeți online prin intermediul propriului site web. Este, de asemenea, cazul în care nu vă puteți stabili securitatea online prin încercare și eroare. Trebuie să o faci bine prima dată, deoarece recuperarea din greșeli este dificilă pentru marile afaceri și practic imposibilă pentru o afacere mică. Dacă reușiți să înșelați securitatea și se știe despre asta, așteptați-vă să vă reconstruiți afacerea și reputația de la zero. În restul acestui articol, vă vom oferi câteva indicații despre cum să evitați soarta respectivă.

1. Nu stocați mai multe informații decât aveți de fapt nevoie

Multe site-uri web au formulare complicate care trebuie completate înainte ca un client să poată face chiar și cele mai elementare achiziții. Adesea, aceste formulare solicită tot felul de informații care nu sunt relevante pentru vânzare. Aceasta este de obicei vina departamentului de marketing care încearcă să obțină demografice sau inutile Informații CRM. Problema este că pre-vânzarea nu este de obicei locul corect pentru a solicita acest tip de date.

Din punct de vedere legal, aveți responsabilitatea de a proteja datele pe care le stocați despre clienții dvs. Există chiar și anumite tipuri de date pe care nu aveți voie să le stocați legal (numere CVS, de exemplu). Chiar și așa, multe site-uri web stochează acele informații pe care nu ar trebui să le stocheze.

Este mult mai bine pentru tine să nu faci asta. În faza de pre-vânzare, puteți pierde clienții cerând prea multe informații. Vor merge într-un loc în care cumpărarea este mai simplă și în care nu simt că se confruntă cu Marea Inchiziție.

Oamenii devin din ce în ce mai preocupați de informațiile pe care le împărtășesc online, astfel încât obiectivul dvs. ar trebui să fie întotdeauna să colectați cantitatea minimă de informații posibilă, deoarece acest lucru vă ajută să creați încredere. Dacă utilizați PayPal sau un serviciu similar pentru a vă procesa plățile, probabil că nu trebuie să colectați informații de la clientul dvs., deoarece PayPal vă furnizează tot ce trebuie să știți pentru a finaliza comanda.

Cu cât stocați mai multe informații, cu atât mai multe sunt disponibile pentru ca cineva să le fure și să le exploateze. Dacă furtul lor este descoperit și urmărit înapoi la dvs., vor apărea mult mai multe probleme care vor apărea ulterior.

2. Dacă colectați informații sensibile, aveți nevoie de SSL

În mod ideal, fiecare site ar trebui să aibă SSL în mod implicit, dar, din păcate, este destul de dificil să se rezolve SSL și există chiar și companii importante de internet care greșesc (de dragul lor, nu le vom numi).

SSL vă oferă o criptare care face mai dificilă (dar nu imposibilă) deturnarea de către cineva sau altelewise interferează cu tranzacția. De asemenea, într-o oarecare măsură protejează informațiile care sunt transmise.

Cea mai importantă caracteristică a SSL - poate chiar mai importantă decât criptarea - este că vă identifică pozitiv site-ul. Chiar și acest lucru nu este perfect, dar este mai bine decât nimic.

3. Luați o decizie conștientă dacă vă procesați propriile tranzacții

Procesarea tranzacțiilor interne vă poate economisi câțiva bani pe fiecare. Dacă efectuați tranzacții cu volum redus, economiile ar putea fi semnificative. De exemplu, PayPal vă va percepe cel puțin 4.5% din valoarea unei tranzacții (suma se reduce cu volume mai mari de tranzacții).

Cu toate acestea, există o mulțime de avantaje în utilizarea externă sistemelor de plăți cum ar fi PayPal, Skrillși WorldPay. Avantajul principal este că nu mai colectați în mod direct informații financiare de la clientul dvs. și, în mod ideal, nu colectați deloc informații. Acest lucru înseamnă că toate sarcinile pentru conformitatea PCI și protecția datelor consumatorilor se încadrează pe umerii serviciului de plată și nu pe umerii dvs. Pentru IMM-uri, aceasta este o povară uriașă ridicată, vă reduce serios răspunderea potențială și simplifică fluxul tranzacțiilor dvs.

Pe de altă parte, au existat povești de groază pentru unii negustori. Principalul vinovat atunci când vine vorba de amestec în afacerile altora este PayPal. Luându-și extrem de serios datoria de a proteja lumea de spălarea banilor, PayPal va îngheța un cont la cel mai mic indiciu că se întâmplă ceva ciudat, iar ridicarea înghețului poate fi o problemă.

O mare parte a problemei PayPal este că este destul de dificil să îi contactați. Un alt lucru infuriant, care nu se limitează în totalitate la PayPal, este deținerea mâinii prea zeloase, în care încearcă să te protejeze prea mult și fără cererea ta de a face acest lucru. Aceasta înseamnă că, dacă încercați să vă conectați la contul dvs. de pe un dispozitiv pe care PayPal nu îl recunoaște, sau dacă ați făcut greșeala prostească de a înregistra un număr de telefon mobil cu acestea, vă puteți bloca din contul dvs. doar călătorind la în altă țară sau schimbarea serviciului de telefonie. Într-o lume în care afacerile devin din ce în ce mai globale și oamenii călătoresc pe plan internațional mult mai des, acest lucru este inacceptabil.

Această problemă poate afecta și alte lucruri pe care se bazează afacerea dvs. Facebook, Twitter, Yahoo, GMail și multe alte servicii pot face cu toții mari dureri de cap atunci când călătoriți în afara zonei obișnuite și nu aveți activat roamingul global pe telefon. Conectarea de pe un dispozitiv necunoscut (sau un dispozitiv familiar cu o cartelă SIM necunoscută) dintr-o locație din afara țării dvs. de origine poate chiar să vă descurce lucrurile, dar cel puțin niciunul dintre aceste servicii nu are control direct asupra fluxului de numerar. Serviciile de plată o fac, deci dacă te blochează, consecințele sunt mai grave.

Cel mai mare motiv pentru a lăsa pe altcineva să gestioneze tranzacțiile pentru dvs.? Clienții sunt renumiți pentru că nu completează corect formularele. Atunci când nu puteți expedia produsul din această cauză, vă vor da vina. Acest lucru poate duce la lucruri urâte, cum ar fi rambursările și, în timp, acest lucru vă poate afecta afacerea și, eventual, și reputația. Predați toate colecțiile de informații unui terț și, din punct de vedere tehnic, sunteți la îndemână.

4. Înainte de a expedia produse, verificați toate detaliile tranzacției

Pentru unele companii, acest lucru poate fi un pic complex. Dacă vindeți produse digitale, cum ar fi cărțile electronice, de exemplu, clienții se așteaptă de obicei să își primească produsul aproape instantaneu. Dacă vindeți mărfuri fizice, aveți puțin mai mult timp pentru a verifica totul și ar trebui să o folosiți.

Asigurați-vă că cantitățile, prețurile și descrierile produselor se potrivesc cu ceea ce ar trebui să corespundă. De asemenea, verificați dacă orice cod de reducere sau cupon este valid.

După cum puteți vedea, menținerea în siguranță nu necesită mult efort sau cheltuială. Practic înseamnă a renunța la obiceiurile marilor corporații. Cu alte cuvinte:

• Nu vă spionați clienții

• Nu colectați informații de care nu aveți strict nevoie

• Protejați informațiile pe care le colectați

• Delegați responsabilitatea conformității, dacă este posibil, utilizând procesarea tranzacțiilor cu terți

• Examinați comenzile înainte de a expedia produse

Singurul lucru pe care trebuie să-l faci întotdeauna este să verifici dacă solicitările de rambursare se potrivesc cu suma tranzacției inițiale. A fost cunoscut faptul că oamenii cumpără la prețul de vânzare și rambursează prețul complet, iar personalul nu observă întotdeauna.

Ce sunt parolele și cum ar trebui să arate o parolă sigura

Pentru azi ar fi bine să vedem ce anume reprezintă o parolă și care sunt cele mai sigure modalități de a alege și de a stoca o parolă. Și nu vorbesc întâmplător de acest clivaj, întrucât alegerea unei parole și păstrarea ei în siguranță reprezintă două lucruri diferite. Nu este suficient să avem o parolă sigură (o să vedem imediat ce presupune acest lucru), dacă nu suntem capabil să o protejăm de privirile indiscrete.

„Parola reprezintă un șir de caractere (litere, cifre, semne, spații) prin intermediul căruia, o persoană (sau organizație) își certifică identitatea și dreptul de a accesa anumite resurse.”

În regulă. Știu că nu este poate cel mai literar mod de concepere a unei definiții, însă scopul acestui mic exercițiu a fost să vă demonstrez că o parolă nu este doar un nume (fie el comun sau propriu) sau o înșiruire de cifre, iar orice abatere de la această definiție de bază a parolei, reprezintă un risc de securitate.

Care sunt parolele necesare unui utilizator obișnuit ?

Parola de logare în sistem

Începând cu Windows NT 3.1 Workstation și apoi Windows 95 pentru utilizatorul individual, s-a încetățenit ideea de logare în sistem. Și asta chiar dacă vorbim de un singur calculator. S-ar zice că a fost primul pas spre securizarea sistemelor. Teoretic. Mulți foloseau, sau încă folosesc celebra parolă „blank”.

Majoritatea au două, trei, patru… zece adrese de mail… că doar nu-i așa… sunt gratuite. Mai delicată este administrarea acestor conturi, alegerea unei întrebări de securitate decente (aici ar fi o altă discuție fiindcă nu este suficient să folosiți o parolă sigură, dacă întrebarea de securitate este una banală).

Parola blogului sau de acces în rețelele sociale

E la modă să avem blog. Cont (cel puțin unul) pe Twitter, pe Facebook, pe Pinterest ori LinkedIn. Cine își bate capul cu parole ? Una și bună să fie. Asta până când ea este „desecretizată” și atunci observați cu mirare că nu vă mai puteți autentifica.

Parola pentru online banking

În număr mai mic, după ce au fost introduse dispozitivele de securizare, mai există cazuri în care utilizatorilor unui astfel de serviciu de online banking li se cere să-și aleagă singuri o parolă. O idee proastă, dacă mă întrebați, deoarece majoritatea vor opta (aproape invariabil) o parolă nesigură. Ce se întâmplă în continuare, este lesne de bănuit și are consecințe dintre cele mai neplăcute.

Cum ar trebui să arate o parolă sigură ?

Bun. Am văzut care ar fi principele parole de care lovește un utilizator obișnuit. Pe locuri, s-a insinuat în discuție subiectul parolelor sigure. A venit vremea să intrăm în detalii. Pas cu pas.

Primul pas: nu folosiți parole doar de dragul parolei. Sau pentru că vă spune cineva.

N-are nici rost. Decât o parolă „12345”, „123456”, „admin” (cu variantele „admin123” sau „admin1), „qwerty”, „password”, „test”… sau orice asemenea năzbâtie, mai bine lipsă.

Pasul doi: parola trebuie să fie UNICĂ

La fel cum anumite persoane își folosesc ziua de naștere „ddmmyyyy” pe post de parolă, de parcă în acea zi s-ar fi dat intersecție în maternități, alții merg pe mâna echipei favorite de fotbal, a actorului preferat, a eroului de benzi desenate care le-a marcat copilăria sau a șefului care le-a mâncat viața. Credeți că sunteți singurul fan al lui Arnold Schwarzenegger, sau vă numărați printre „cei aleși” care reușesc să scrie corect numele starului american ? UNICĂ înseamnă INVENTATĂ, CREATĂ de voi.

Pasul trei: parola NU TREBUIE SĂ AIBĂ LEGĂTURĂ CU VOI

Începând cu persoanele care își folosesc id-ul de messenger pe post de parolă, mergând până la numele cățelului, al peștișorului, al soțului, al copilului / depinde de fiecare ce lighioană are în grijă, asemenea detalii sunt foarte ușor de aflat și nu garantează securitatea. Veți spune că mă repet și că o parolă unică exclude o legătură directă cu persoana voastră. Goleo, mascota campionatului mondial din Germania, era unic și totuși… cunoscut de toată lumea.

Pasul patru: parola trebuie să fie UȘOR DE MEMORAT

Aici fac o precizare suplimentară. Chiar dacă aveți 15-20 de parole, nu este nevoie să le țineți minte de toate, dar măcar una singură, trebuie să fie ușor de memorat. Așa numit-a „master password”. Există și-o axiomă: „Hard to guess, easy to remember”.

Pasul cinci: NU FOLOSIȚI PAROLE MAI SCURTE DE 8 CARACTERE

Cu 8 caractere (2 la puterea a treia) se poate genera o parolă de aproximativ 50 de biți. V-am lămurit buștean, nu ? Hai să punem altfel problema. O parolă de 4 caractere, formată doar din cifre (cazul PIN-urilor) are o valoare de 10,12 sau maxim 14 biți, insuficientă cât să reziste unui număr mare de încercări.

Pasul șase: LITERE, CIFRE, SEMNE

Chiar și spații, acolo este permis. Paranteză. Prin definiție, password ne duce cu gândul la existența unu singur cuvânt (eng. word), însă dacă termenul este fracturat prin introducea unor spații, parola nu mai fi formată doar dintr-un cuvânt, ci din mai multe. În acest caz, denumirea corectă este de passphrase. Conform logicii, passphrase (frază parolă) este considerată mai sigură, decât varianta fără spații (password).

Ce ar trebuie să știe orice utilizator care încearcă să-și aleagă a parolă potrivită, este că nu trebuie să se ferească în a utiliza semne sau caractere speciale:

!@ # $ % ^ & * ( ) _ + = –] [{ } | ‘ ” ; : , . < > / ? – ”„

Pasul șapte: FIECARE CONT CU PAROLA LUI

Să presupunem că ați reușit să vă găsiși parola perfectă. Mă bucur pentru voi, dar dacă o veți folosi pentru trei, cinci, zece conturi, inclusiv ca să vă logați pe blogul vecinei de șase (care păstrează aceste date într-un fișier text, neprotejat și necriptat), parola voastră de un milion de dolari, tocmai ce a devenit inutilă. Și trebuie s-o luați de capăt. Bine, asta dacă mai aveți cu ce.

Să alegem o parolă sigură

Graham Cluley, unul dintre cei mai renumiți experți la nivel mondial în problema virușilor și spam-ului, ne demonstrează cum o parolă poate fi sigură și ușor de reținut în același timp. Nu degeaba l-or fi angajat cei de la Sophos „Senior Technology Consultant”. El sinterizează cele explicate de mine anterior și le pune într-o formă ceva mai atractivă, pentru că nu-i așa, o parolă e ceva destul de abstract, de unde toată această demonstrație.

Cum deosebim paginile sigure de fake-uri

In primul rand conteaza foarte mult experienele persoanelor din jurul tau; fa un mic research printre prieteni si cunostinte. Poti chiar sa si intrebi pe facebook pareri pro si contra. Oamenii care au avut experiente urate iti vor povesti si te vor atentiona de ce sa te feresti. Daca prietenii tai nu cunosc

site-ul cauta produsele in blogosfera, de regula bloggerii fac poze de detaliu si dat si aspectele negative daca e cazul.

cauta informatii despre numele magazinului si probleme. Eventual ce poti sa faci este sa cauti in browserul tau asa: ,, RECLAMATII/ PROBLEME/ RECENZII si pui numele magazinului.

daca vizual site-ul iti inspira incredere e ok. Eu de exemplu nu as cumpara niciodata de pe un site care nu are poze la rezolutie ok, care nu permite zoom pozelor, care nu foloseste persoane reale in promovare ci manechie de plastic, care nu are un contact si nr de telefon sau unde nu pot sa gasesc review-uri chiar si pe pag de FB a site-ului. Conteaza foarte mult ca site-ul sa aibe un aspect ingrijit iar pozele sa se incarce repede.

Conexiune securizata HTTPS – este cel mai important lucru pe care un magazin online trebuie sa-l aiba: o conexiune securizata HTTPS, fie pe toate paginile magazinului, fie doar in zona cosului de cumparaturi si zona de finalizare a comenzii. Cauta in bara de adresa a sitului simbolul lacatului inchis sau asigura-te ca adresa paginii curente incepe cu 'https://', cu 's'.

ATENTIE: Simbolul lacatul plasat in zona de afisare a sitului in browserul web NU reprezinta conexiune securizata. Oricine poate pune imaginea unui lacat pe site. Click pe lacatel in zona barei de adresa (URL) va afisa cateva informatii suplimentare despre certificatul SSL de securizare al siteului respectiv, cea mai importanta informatie fiind institutia care a eliberat acel certificat

Fii atent ce informatii oferi atunci cand plasezi comanda – esti la pasul in care vrei sa dai comanda si trebuie sa completezi datele persoanele si cateva info necesare efectuarii platii. Nu exista motiv pentru care ti-ar cere mai mult decat numele, adresa de livrare si datele cardului. Nu da date personale, CNP-ul, daca chiar e nevoie asigura-te ca stii de ce il dai.

Verifica cateva date ale magazinului care ar trebui sa fie publice, ca de exemplu: un magazin online trebuie sa afiseze pe site datele de contact ale comerciantului, numele firmei care administreaza siteul, numarul unic de inregistrare fiscala, adresa fizica, numarul de telefon. Puteti verifica aceste date pe site-ul asp.gov.md

Inainte de a plasa comanda verifica numarul de telefon, chiar emailul daca nu te grabesti. Trimite un email. Un magazin care se respecta iti va raspunde in cel mai scurt timp.

Foloseste aplicatiile magazinului daca acesta are unele.

Fii atenta si la preturi; preturile foarte mici cu exceptia celor de la promotiile oficiale ar trebui sa iti ridice un semnal de alarma ,, de ce sunt ami ieftine aici" calitatea, materialul etc.

Daca ai verificat toate acestea si te-ai decis sa faci shopping verifica urmatoarele: ca ai antivirus pe telefon, ca functioneaza, ca ai o parola puternica, ca nu platesti de pe calculatoarele publice sau wifi;

cumpara cu verificare colet si plata ramburs;

verifica la cateva zile dupa ce ai platit extrasul de cont.Asta in cazul in care platesti cu cardul;

verifica politica de retur si ce presupune asta sa fii la curent cu ce s-ar intampla daca esti sau nu nemultumit. In cat timp iti recuperezi banii, pot fi su nu produsele schimbate. Este sau nu returul gratuit.

Securitatea e-mail-lului și a mesageriilor.

Chat-ul live, mesageria social media, aplicatiile de project management – sunt doar cateva dintre mijloacele pe care companiile le folosesc acum pentru a pastra legatura cu clientii, angajatii si furnizorii. Multi se asteptau ca aceste noi canale sa duca la disparitia emailului, scazand astfel importanta securitatii emailurilor. Totusi, nimic nu ar putea fi mai departe de adevar. Si iata de ce:

1. Emailul rămâne mijlocul de comunicare favorit in afaceri

Companiile au mai multe mijloace digitale prin care pot comunica cu clientii. Dar niciuna dintre acestea nu a reusit sa elimine emailul de pe pozitia #1. Peste 300 de miliarde de e-mailuri sunt trimise si primite in fiecare zi.

Asemenea cifre il fac in mod natural cea mai populara tinta pentru atacurile cibernetice. De la furt de parole si atacuri de tip „man-in-the-middle", pana la phishing si fraudari de diverse tipuri, emailul ramane unul dintre cele mai vulnerabile canale de comunicare in afaceri. O mare parte din programele malware, inclusiv cele de tip ransomware, sunt raspandite prin e-mail.

2. Emailul este formal, dar totusi personal

Emailul este un instrument esential de comunicare pentru mediul pentru afaceri. Este mai personal si mai rapid decat instrumentele colaborative de project management, dar mai formal decat chat-ul live si mesageria social media. Atacatorii stiu ca este posibil sa obtina informatiile dorite daca folosesc emailul in loc de alte mijloace de comunicare mai putin adoptate.

3. Este operat manual

Emailul este operat manual de catre utilizatorii sai. Depinde in primul rand de oameni sa citeasca mesaje, sa raspunda, sa descarce atasamente si sa faca click pe linkuri. Filtrele de spam si software-ul antimalware pot bloca o mare parte din e-mailurile nedorite dar cu toate acestea, unele emailuri cu malware reusesc sa treaca de sistemele de securitate.

4. Este o sursa valoroasa de informatii sensibile

Emailul permite organizatiilor diseminarea rapida si eficienta a unei game largi de informatii. Puteti trimite orice, de la invitatii la apeluri video si detalii bancare, pana la documente privind strategia companiei si contracte de vanzare.

Aceasta versatilitate si simplitate fac posibila transmiterea pe neobservate a diverselor amenintari. In plus, serverele de email reprezinta un rezervor valoros de informatii despre companie si date personale.

5. Se afla in prima linie de atac si aparare

Daca infractorii cibernetici se gandesc sa initieze un atac asupra companiei dvs., emailul va fi probabil prima lor tinta. Daca nu se implementeaza instrumente si controale adecvate pentru securitatea emailurilor orice alte masuri de securitate cibernetice pe care le-ati introdus sunt inadecvate.

6. Kit-uri de Phishing si Phishing-as-a-Service

Proliferarea kiturilor de Phishing si Phishing-as-a-Service a conferit viteza si amploare amenintarilor cibernetice. Un atacator nu mai trebuie sa aiba abilitati tehnice pentru a dezvolta si implementa un atac de phishing. O persoana cu cunostinte digitale minime poate initia un atac, achizitionand pur si simplu un kit disponibil la un pret modest.

Acum sunt disponibile servicii de phishing, Phishing-as-a-Service, de unde infractorii isi pot alege pagina de phishing dorita si servicii hosting pentru o luna! Printre paginile clonate se regasesc: Sharepoint, Office 365, LinkedIn, OneDrive, Google, Adobe si multe altele.

7. Cloud-based computing

Corporatiile au recunoscut enormele avantaje de eficienta de care beneficiau facand trecerea de la o configuratie locala la una bazata pe cloud. Serverele de email anterior on-site, au fost mutate in cloud. Odata cu aceasta a venit pierderea perimetrului retelei traditionale.

Pentru ca un atacator sa aiba acces la serverul dvs. de e-mail nu mai trebuia sa va compromita mai intai reteaua locala. Acesta ar putea sa va fure datele de autentificare Microsoft 365 si ulterior sa stabileasca reguli care monitorizeaza si redirectioneaza e-mailurile. Le-ar oferi informatii despre afacerea dvs., clientii, vanzatorii si angajatii dvs.

8. Atacuri mai sofisticate

In trecut, programele malware foloseau un model de executie previzibil ale carui semnaturi puteau fi identificate de motoarele antivirus. In prezent, programele malware utilizeaza algoritmi si formule sofisticate pentru a evita detectarea de catre motoarele traditionale bazate pe semnaturi. Prezinta o gama larga de comportamente in functie de mai multi factori, inclusiv mediul in care este implementat.

E-mailurile de tip phishing folosesc mai multe tactici pentru a se sustrage detectarii, inclusiv variatii ale expeditorilor, subiectelor, textului si a adresei URL. Un atacator poate juca rolul mai multe parti diferite in cadrul aceleiasi campanii de phishing pentru a face mesajul mai credibil pentru o victima.

9. Ransomware

Ransomware-ul a afectat lumea intr-un mod fara precedent. Pierderea accesului la sisteme si date critice a impins multe organizatii sa plateasca rascumpararea. Rezultatele acestui tip de atac sunt perioadele de nefunctionare (downtime), pierderea increderii clientilor, pierderea datelor, pierderi financiare si afectarea reputatiei.

Ransomware-ul este propagat in principal prin e-mail. Orice incercare de prevenire a acestor atacuri trebuie sa tina cont de importanta securitatii emailului.

10. Cresterea amenintarilor in contextul pandemiei

Un studiu recent al Cloudflare arata ca amenintarile online au crescut cu 500% peste nivelurile obisnuite la scurt timp dupa pandemie. Schimbarea dramatica a mediului de lucru la distanta a creat noi vulnerabilitati care nu existau inainte. Mai mult, aceste schimbari au trebuit sa aiba loc in cateva saptamani iar unele companii nu aveau experienta anterioara in gestionarea sau sprijinirea unei forte de munca la distanta.

Atacatorii au devenit mai agresivi in timp ce au incercat sa exploateze noi oportunitati, cum ar fi conexiunile nesigure, aplicatiile prost configurate si angajatii neinformati. Atacurile de tip phishing au explodat, iar acest lucru a amplificat si mai mult importanta securitatii e-mailurilor.