Tip malware	Descriere
troian	Software rău intenționat care execută o funcție specifică, nedorită și adesea dăunătoare pentru computer.
virus	Program malware care execută cod arbitrar și instalează copii ale acestuia în memoria computerului infectat. Scopul principal al acestui malware este de se a reproduce automat de la sistem la sistem în întreaga rețea.
vierme	Tip de malware care nu se auto-replică. Conține adesea coduri rău intenționate care sunt concepute pentru a arăta ca altceva, cum ar fi o aplicație sau un fișier legitim. Atacă dispozitivul din interior.
spyware	Programe malware utilizate pentru a colecta informații despre un utilizator și, fără consimțământul utilizatorului, trimit informațiile către o altă entitate.
adware	Programe malware care afișează de obicei ferestre pop-up enervante pentru a genera venituri pentru autorul său.
phishing	Malware care încearcă să convingă oamenii să divulge informații sensibile.
scareware	Programe malware care includ programe de înșelătorie ce utilizează ingineria socială pentru a șoca, a provoca anxietate sau a determina sentimentul unei amenințări. În general, se adresează unui utilizator naiv.
rootkit	Program malware care este instalat pe un sistem compromis și oferă acces privilegiat hackerului.
ransomware	Programe malware care refuză accesul la sistemul informatic infectat și solicită o plată pentru eliminarea restricției.

Termen	Definiție
Dumpster diving	Acesta este un tip de atac în persoană în care un atacator caută prin coșurile de gunoi pentru a descoperi documente confidențiale.
Furtul de identitate	Acest tip de atac este acela în care un atacator se preface că este altcineva (de exemplu, nou angajat, alt angajat, vânzător sau angajat al companiei partenere etc.) pentru a câștiga încrederea unei victime.
phishing	Un atacator trimite un e-mail fraudulos deghizat ca provenind dintr-o sursă legitimă și de încredere pentru a păcăli destinatarul să instaleze malware pe dispozitivul său sau să partajeze informații personale sau financiare (de exemplu, numărul de cont bancar și codul de acces).
Spear phishing	Un atacator creează un atac de phishing țintit special pentru o persoană sau organizație.
Baiting	Un atacator lasă o unitate flash infectată cu malware într-o locație publică (de exemplu, o toaletă corporativă). O victimă găsește unitatea și o introduce, fără a suspecta ceva, în laptopul corporativ, instalând involuntar malware.
Social Engineering	Uneori numit "Quid pro quo" - un atacator solicită informații personale de la cineva, în schimbul a ceva (ex. un cadou).
Pretexting	Atacator care pretinde că are nevoie de date personale sau financiare pentru a confirma identitatea destinatarului.

Test de bază pentru securitate cibernetică

1. Care dintre următoarele acțiuni ar trebui să faceți pentru a restricționa accesul la fișierele și dispozitivele dvs.?
A. Actualizați software-ul o dată pe an.
B. Partajați parolele numai cu colegii în care aveți încredere.
C. Cereți membrilor personalului să acceseze informații printr-o rețea Wi-Fi deschisă.
D. Utilizați autentificarea cu mai mulți factori.

2. Copierea de rezervă a fișierelor importante offline, pe un hard disk extern sau în cloud, vă va ajuta să vă protejați afacerea în cazul unui atac cibernetic. Adevărat sau fals?
Adevărat
Fals

3. Care este cel mai bun răspuns pentru care oamenii dintr-o afacere ar trebui să fie responsabili pentru securitatea cibernetică?
A. Proprietarii de afaceri. Ei conduc afacerea, așa că trebuie să cunoască elementele de bază ale securității cibernetice și să le pună în practică pentru a reduce riscul atacurilor cibernetice.
B. Specialiști IT, pentru că sunt în cea mai bună poziție pentru a cunoaște și promova securitatea cibernetică în cadrul unei afaceri.
C. Managerii, deoarece sunt responsabili pentru a se asigura că membrii personalului urmează practicile corecte.
D. Toți membrii personalului ar trebui să cunoască câteva elemente de bază privind securitatea cibernetică pentru a reduce riscul atacurilor cibernetice.

4. Infractorii cibernetici vizează doar companiile mari. Adevărat sau fals?
Adevărat
Fals

5. Care dintre următoarele este cel mai bun răspuns despre cum să vă securizați routerul?
A. Schimbați numele și parola implicite ale routerului.
B. Opriți gestionarea de la distanță a routerului.
C. Deconectați-vă ca administrator odată ce routerul este configurat.
D. Toate cele de mai sus.

Test de phishing

Primești un e-mail sau un text care pare să provină de la unul dintre furnizorii companiei tale. Vă solicită să faceți clic pe un link pentru a vă actualiza contul de afaceri. Ar trebui să dai clic? Probabil că nu. Aceasta ar putea fi o încercare de phishing. Pentru a afla cât de multe știi despre phishing, alege cel mai bun răspuns pentru fiecare întrebare sau afirmație.

1. Care dintre aceste afirmații este corectă?
R. Dacă primiți un e-mail care pare să provină de la cineva cunoscut, puteți face clic pe orice link, atâta timp cât aveți un dispozitiv de blocare a spam-ului și protecție antivirus.
B. Puteți avea încredere că un e-mail vine cu adevărat de la un client dacă folosește logo-ul clientului și conține cel puțin un fapt despre client despre care știți că este adevărat.
C. Dacă primiți un mesaj de la un coleg care are nevoie de parola dvs. de rețea, nu trebuie să îl transmiteți niciodată decât dacă colegul spune că este o urgență.
D. Dacă primiți un e-mail de la Resurse Umane care vă solicită să furnizați informații personale imediat, ar trebui să îl verificați mai întâi pentru a vă asigura că sunt cine spun că sunt.

2. Un e-mail de la șeful tău solicită numele, adresele și informațiile despre cardul de credit ale clienților de top ai companiei. E-mailul spune că este urgent și vă rugăm să răspundeți imediat. Ar trebui să răspunzi imediat. Adevărat sau fals?
Adevărat
Fals

3. Primiți un mesaj text de la un furnizor care vă cere să faceți clic pe un link pentru a vă reînnoi parola, astfel încât să vă puteți conecta la site-ul său web. Ar trebui:
A. Răspundeți la text pentru a confirma că într-adevăr trebuie să vă reînnoiți parola.
B. Ridicați telefonul și sunați la furnizor, folosind un număr de telefon despre care știți că este corect, pentru a confirma că cererea este reală.
C. Faceți clic pe link. Dacă vă duce la site-ul furnizorului, atunci veți ști că nu este o înșelătorie.

4. Autentificarea prin e-mail poate ajuta la protejarea împotriva atacurilor de tip phishing. Adevărat sau fals?
Adevărat
Fals

5. Dacă te îndrăgostești de o înșelătorie de tip phishing, ce ar trebui să faci pentru a limita daunele?
A. Ștergeți e-mailul de phishing.
B. Deconectați computerul. Acest lucru va scăpa de orice malware.
C. Schimbați orice parole compromise.

Test de securitate fizică

Securitatea fizică puternică este o parte importantă a securității cibernetice. Un furt, un laptop pierdut, un dispozitiv mobil furat sau o unitate flash deplasată poate avea consecințe grave.
Pentru a afla cât de multe știi despre securitatea fizică, selectează răspunsul corect pentru fiecare întrebare.

1. Promovarea securității fizice include protejarea:
A. Doar dosare de hârtie.
B. Numai fișiere pe hârtie și orice computer pe care stocați copii electronice ale acelor fișiere.
C. Numai fișiere de hârtie, unități flash și dispozitive de la punctul de vânzare.
D. Toate cele de mai sus plus orice alt dispozitiv cu informații sensibile pe acesta.

2. Fișierele de hârtie care conțin informații sensibile trebuie aruncate într-un coș de gunoi încuiat. Adevărat sau fals?
Adevărat
Fals

3. Când apăsați tasta „Ștergere", înseamnă că un fișier este eliminat automat din computer. Adevărat sau fals?
Adevărat
Fals

4. Care dintre aceste afirmații este adevărată?
R. Cel mai bine este să utilizați autentificarea cu mai mulți factori pentru a accesa zone ale rețelei de afaceri cu informații sensibile.
B. Ar trebui să utilizați aceeași parolă pentru dispozitivele cheie de afaceri pentru a garanta că angajații de nivel înalt le pot accesa în caz de urgență.
C. Cel mai bun mod de a proteja datele de afaceri este să vă asigurați că nimeni nu pierde niciun dispozitiv.
D. Nu ar trebui să limitați încercările de conectare pe dispozitivele cheie ale afacerii, deoarece dacă nu vă blocați pentru prea multe încercări incorecte, nu veți putea accesa conturile.

5. Doar persoanele cu acces la date sensibile trebuie să fie instruite cu privire la importanța securității fizice a fișierelor și echipamentelor. Adevărat sau fals?
Adevărat
Fals

Test de ransomware

Cineva din compania ta primește un e-mail. Pare legitim, dar cu un singur clic pe un link sau o descărcare a unui atașament, toată lumea este blocată din rețea. Cum identifici ransomware-ul și ce ar trebui să faci pentru a-ți proteja afacerea?
Pentru a afla cât de multe știți despre ransomware, selectați răspunsul corect pentru fiecare întrebare sau afirmație.

1. Ce este ransomware-ul?
A. Software-ul care infectează rețelele de computere și dispozitivele mobile pentru a vă ține ostatici datele până când trimiteți bani atacatorilor.
B. Echipamente informatice pe care infractorii ți le fură și nu se vor întoarce până nu le plătești.
C. Software utilizat pentru a vă proteja computerul sau dispozitivul mobil de viruși dăunători.
D. O formă de criptomonedă.

2. Fișierele de rezervă locale – salvate pe computerul dumneavoastră – vă vor proteja datele împotriva pierderii într-un atac ransomware. Adevărat sau fals?
Adevărat
Fals

3. Care dintre acestea descrie cel mai bine modul în care infractorii declanșează atacuri ransomware?
A. Trimiterea unui e-mail înșelătorie cu link-uri sau atașamente care vă pun în pericol datele și rețeaua.
B. Intrarea în serverul dvs. prin vulnerabilități și instalarea de programe malware.
C. Folosind site-uri web infectate care descarcă automat software rău intenționat pe computer sau dispozitiv mobil.
D. Toate cele de mai sus.

4. Dacă întâmpinați un atac ransomware, primul lucru pe care ar trebui să-l faceți este să plătiți răscumpărarea. Adevărat sau fals?
Adevărat
Fals

5. Setarea software-ului pentru actualizarea automată este o modalitate prin care vă puteți proteja afacerea de ransomware. Adevărat sau fals?
Adevărat
Fals

Test de atac securizat de la distanță

Știți ce standarde de securitate ar trebui să urmați înainte de a vă conecta la rețeaua companiei de la distanță?
Pentru a vă testa înțelegerea securizării accesului la distanță, selectați răspunsul corect pentru fiecare întrebare sau afirmație.

1. Înainte de a vă conecta de la distanță la rețeaua companiei, dispozitivul dvs. personal trebuie să îndeplinească aceleași cerințe de securitate ca și dispozitivele emise de companie. Adevărat sau fals?
Adevărat
Fals

2. Care este o modalitate obișnuită de a ajuta la protejarea dispozitivelor conectate la rețeaua companiei?
A. Folosiți numai laptopuri și alte dispozitive mobile cu criptare completă a discului.
B. Modificați setările smartphone-ului pentru a permite dispozitivelor să se conecteze automat la Wi-Fi public.
C. Permiteți oaspeților și clienților să folosească același Wi-Fi securizat pe care îl utilizați.
D. Folosiți parola presetată a routerului, astfel încât să nu o uitați.

3. Păstrarea numelui implicit al routerului dvs. va ajuta profesioniștii în securitate să-l identifice și, astfel, vă va proteja securitatea rețelei. Adevărat sau fals?
Adevărat
Fals

4. Criptarea WPA2 și WPA3 sunt standardele de criptare care vor proteja informațiile trimise printr-o rețea fără fir. Adevărat sau fals?
Adevărat
Fals

5. Care dintre următoarele descrie cel mai bun mod de a vă asigura că accesați în siguranță rețeaua companiei de la distanță?
A. Citiți cu atenție politicile de securitate cibernetică ale companiei dvs.
B. Utilizați VPN atunci când vă conectați de la distanță la rețeaua companiei.
C. Utilizați parole de rețea unice și complexe și evitați stațiile de lucru deschise și nesupravegheate.
D. Faceți toate cele de mai sus.

Test pentru inselatorii de asistență tehnică

Primiți un apel telefonic, o fereastră pop-up sau un e-mail care vă anunță că există o problemă cu computerul dvs. Ce ai face mai departe?
Pentru a vă testa înțelegerea înșelătoriilor de asistență tehnică, alegeți răspunsul corect pentru fiecare întrebare sau afirmație.

1. Care dintre următoarele scenarii NU descrie o înșelătorie de suport tehnic?
R. Cineva sună și vă spune că a găsit viruși pe computerul dvs., apoi vă solicită informații despre cardul de credit pentru a vă putea factura pentru serviciile de asistență tehnică.
B. În timp ce navigați online, apare un mesaj urgent care vă spune că există o problemă cu computerul dvs. și vă direcționează către un site web pentru a plăti pentru serviciile de asistență tehnică.
C. Un apelant vă cere să îi acordați acces de la distanță la computerul dvs. pentru a remedia o problemă în computer.
D. Plătiți un profesionist de securitate de încredere pentru a vă verifica rețeaua pentru intruziuni, iar profesionistul vă spune că rețeaua dvs. are o problemă care trebuie remediată.

2. Adevărat sau fals? Puteți evita înșelătoriile luând numai apeluri de asistență tehnică de la companii de tehnologie binecunoscute.
Adevărat
Fals

3. Care dintre aceste răspunsuri descrie cel mai bun mod de a vă proteja împotriva înșelătoriilor de suport tehnic?
A. Utilizați o parolă unică pentru fiecare cont.
B. Scanați computerul pentru orice software necunoscut.
C. Închideți apelantii care spun că computerul dvs. are o problemă.
D. Toate cele de mai sus.

4. Adevărat sau fals? Întreprinderile mici ar trebui să se concentreze mai mult pe alte amenințări la adresa securității cibernetice, deoarece escrocii de asistență tehnologică vizează de obicei doar companiile mari.
Adevărat
Fals

5. Care este cel mai bun mod de a vă proteja împotriva virușilor sau a altor amenințări de securitate?
A. Sună-ți compania de software de securitate pentru a revizui pașii pe care i-a luat pentru a configura protecția împotriva virușilor și ce altceva a făcut sau poate face pentru a-ți proteja afacerea.
B. Angajați o companie nouă care a făcut efortul de a vă alerta cu privire la virușii din sistemul dvs. și se oferă să vă ajute să-i remediați.
C. Instalați un nou software de protecție împotriva virușilor pe care îl găsiți online.
D. Schimbați parola rețelei.

Test de securitate pentru furnizori

Un furnizor a cărui rețea este conectată la a ta este piratat. Rezultatul: datele dvs. de afaceri și informațiile personale ale clienților dvs. au ajuns în mâini greșite - punându-vă afacerea și clienții în pericol.
Furnizorii dvs. pot juca un rol important în păstrarea în siguranță a informațiilor companiei dvs. Când selectați un furnizor, știți care sunt întrebările potrivite de adresat? Faceți acest test pentru a vă testa cunoștințele de securitate ale furnizorului.

1. Ce pași ar trebui să luați atunci când selectați furnizorii care vor avea acces la informațiile dvs. sensibile? Alegeți cel mai bun răspuns.
A. Includeți prevederi pentru securitate în contractele dvs. cu furnizorii, cum ar fi un plan de evaluare și actualizare a controalelor de securitate.
B. Faceți afaceri numai cu furnizori cunoscuți.
C. Asigurați-vă că furnizorii dvs. înțeleg regulile dvs. de conformitate.
D. Confirmați că furnizorul înțelege importanța securității cibernetice.

2. Oricui are acces la rețeaua dvs. de afaceri ar trebui să li se solicite să folosească o parolă puternică. Cât de lungă ar trebui să fie o parolă puternică?
A. Parolele trebuie să aibă cel puțin 8 caractere, cu un amestec de numere, simboluri și litere mari și mici.
B. Parolele trebuie să aibă cel puțin 5 caractere cu un amestec de numere, simboluri și litere mari și mici.
C. Parolele trebuie să aibă cel puțin 12 caractere, cu un amestec de numere, simboluri și litere mari și mici.
D. Parolele trebuie să aibă cel puțin 10 caractere cu un amestec de numere, simboluri și litere mari și mici.

3. Solicitarea furnizorilor să folosească autentificarea cu mai mulți factori pentru a vă accesa rețeaua face ca utilizatorii să facă un pas suplimentar dincolo de autentificarea cu o parolă. Adevărat sau fals?
Adevărat
Fals
4. Criptarea puternică configurată corespunzător – recomandată pentru orice dispozitive care se conectează de la distanță la rețeaua dumneavoastră – vă poate ajuta să detectați atacurile cibernetice în sistemul dumneavoastră. Adevărat sau fals?
Adevărat
Fals

5. Ce ar trebui să faceți dacă un furnizor are o încălcare care afectează datele dvs. de afaceri? Alegeți cel mai bun răspuns.
A. Schimbați toate parolele de rețea.
B. Opriți toate computerele și dispozitivele.
C. Asigurați-vă că furnizorul remediază vulnerabilitățile și se asigură că informațiile dvs. vor fi în siguranță pe viitor.
D. Dezactivați sistemele de autentificare cu mai mulți factori.

4. Accesati site-ul securizat din adresa de mai jos si realizati chestionarul phishing online disponibil https://phishingquiz.withgoogle.com/