FREEDIVISION

SOLUTION GUIDE

FreeDivision.io PhishingGym

Human Risk Management

Systematické snižování lidského rizika prostřednictvím bezpečnostní osvěty a vzdělávání.

Proč organizace potřebují simulační kampaně a bezpečnostní vzdělávání

Kybernetické útoky se stále častěji zaměřují na lidské chování místo technických slabin. Útočníci využívají důvěry, časového tlaku, autority nebo zvědavosti zaměstnanců a vytvářejí scénáře, které jsou stále obtížněji rozpoznatelné.

Moderní phishing už dávno není jen e-mail s gramatickými chybami nebo podezřelým odkazem. Současné kampaně využívají informace z veřejně dostupných zdrojů, umělou inteligenci i znalost firemního prostředí. Výsledkem jsou zprávy, které působí důvěryhodně a často napodobují běžnou interní komunikaci.

Technologie dokážou významnou část těchto útoků zastavit, žádné řešení však nedokáže zcela nahradit správné rozhodnutí uživatele. Právě proto představuje lidský faktor jednu z nejdůležitějších součástí bezpečnostní architektury.

Účinné vzdělávání nespočívá v jednorázovém školení jednou za rok. Mnohem vyšší efekt přináší pravidelné procvičování prostřednictvím realistických scénářů, okamžitá zpětná vazba po rizikovém chování a krátké vzdělávací moduly, které nenarušují běžnou práci zaměstnanců.

FreeDivision.io PhishingGym je postaven právě na tomto principu. Místo jednorázové povinnosti vytváří dlouhodobý program, který pomáhá budovat bezpečnostní návyky, průběžně měřit jejich rozvoj a systematicky snižovat pravděpodobnost úspěšného phishingového útoku.

Executive Summary

Technologie samy o sobě nedokážou odstranit lidské riziko. Phishing, sociální inženýrství a manipulace uživatelů stále patří mezi nejúčinnější cesty, jak obejít technická bezpečnostní opatření.

FreeDivision.io PhishingGym proto propojuje realistické phishingové simulace, okamžitou zpětnou vazbu, mikroškolení, navazující vzdělávání a manažerský reporting do dlouhodobého programu rozvoje bezpečnostního povědomí.

Organizace tak může průběžně měřit odolnost zaměstnanců, identifikovat rizikové skupiny a systematicky snižovat lidské riziko. Řešení lze provozovat samostatně nebo propojit s platformou FreeDivision.io Advanced.

Proměňte zaměstnance v aktivní součást obrany organizace.

Jak řešení funguje

FreeDivision.io PhishingGym je navržen jako dlouhodobý program rozvoje bezpečnostního povědomí zaměstnanců. Nejde o jednorázové testování ani o pravidelné rozesílání phishingových e-mailů. Cílem je systematicky budovat správné bezpečnostní návyky, průběžně měřit jejich rozvoj a poskytovat organizaci přehled o lidském riziku.

Řešení propojuje phishingové simulace, okamžitou zpětnou vazbu, krátká vzdělávací školení a manažerský reporting do jednoho uceleného procesu. Jednotlivé části na sebe navazují a vytvářejí přirozený cyklus neustálého zlepšování.

Simulace reálných útoků

Program začíná pravidelnými phishingovými kampaněmi, které odpovídají aktuálním metodám používaným útočníky.

Scénáře jsou navrženy tak, aby připomínaly běžnou firemní komunikaci a reflektovaly současné trendy v oblasti phishingu a sociálního inženýrství. Zaměstnanci se tak setkávají se situacemi, které mohou nastat i v reálném provozu, aniž by byla narušena jejich každodenní práce.

Kampaně lze cílit na celou organizaci nebo na vybrané skupiny uživatelů podle jejich pracovního zařazení, lokality či úrovně rizika.

Okamžitá zpětná vazba

Největší vzdělávací efekt vzniká bezprostředně po chybě.

Pokud uživatel během simulace klikne na odkaz, otevře přílohu nebo provede jinou rizikovou akci, okamžitě obdrží stručné vysvětlení situace a doporučení, jak podobný útok v budoucnu rozpoznat.

Tento přístup mění chybu v příležitost ke vzdělávání. Uživatel získává zpětnou vazbu v okamžiku, kdy si nejlépe pamatuje své rozhodnutí, což významně zvyšuje efektivitu učení.

Mikroškolení

Největší vzdělávací efekt vzniká bezprostředně po chybě. Pokud uživatel během simulaNa okamžitou zpětnou vazbu navazují krátké vzdělávací moduly zaměřené na konkrétní typ rizika.

Mikroškolení jsou navržena tak, aby jejich absolvování trvalo přibližně jednu až dvě minuty. Zaměstnanci si mohou rychle osvojit správné bezpečnostní postupy, aniž by byli výrazně vyrušeni z běžné práce.

Tento způsob vzdělávání přináší vyšší zapojení uživatelů než tradiční e-learningové kurzy a podporuje pravidelné upevňování bezpečnostních návyků.

Navazující vzdělávání

Vybraná témata lze dále rozšířit prostřednictvím delších školení a tematických kurzů.

Organizace může vzdělávání přizpůsobit jednotlivým rolím, oddělením nebo aktuálním bezpečnostním rizikům. Zaměstnanci tak získávají znalosti odpovídající jejich pracovní náplni i úrovni odpovědnosti.

Tento přístup umožňuje vytvářet dlouhodobý vzdělávací program namísto jednorázových školení.

Vyhodnocování a reporting

Každá phishingová kampaň poskytuje cenné informace o úrovni bezpečnostního povědomí organizace.

FreeDivision.io PhishingGym průběžně vyhodnocuje výsledky jednotlivých kampaní, sleduje úspěšnost školení a identifikuje oblasti, které vyžadují další pozornost.

Klíčové schopnosti řešení

FreeDivision.io PhishingGym spojuje simulace, vzdělávání a měření lidského rizika do jednoho dlouhodobého programu.

Realistické simulace

Realistické phishingové kampaně lze přizpůsobit konkrétním skupinám uživatelů a aktuálním hrozbám.

Okamžitá mikroškolení a vzdělávání

Na rizikové chování navazuje okamžitá zpětná vazba, krátké mikroškolení a podle potřeby i další tematické vzdělávání.

Manažerský přehled

Management získává přehled o vývoji výsledků, rizikových skupinách a efektivitě vzdělávání prostřednictvím dashboardů a reportingu.

Integrace do FreeDivision.io Advanced

Výsledky lze propojit s řešením FreeDivision.io Advanced, vyhodnocovat je jako součást centrálně řízených bezpečnostních operací a využít jako podklady pro audit, compliance, NIS2 a další interní či regulatorní procesy.

Varianty řešení

FreeDivision.io PhishingGym je navržen jako flexibilní služba, kterou lze přizpůsobit velikosti organizace, interním kapacitám i způsobu řízení bezpečnostního vzdělávání. Zákazníci si mohou zvolit model, který nejlépe odpovídá jejich potřebám – od samostatné správy platformy až po plně řízený program bezpečnostní osvěty.

[STARTER]

Platforma připravená pro vlastní správu

Varianta Starter je určena organizacím, které chtějí provozovat phishingové simulace a vzdělávací program vlastními silami, ale očekávají odbornou podporu při zavedení řešení.

Součástí dodávky je implementace platformy, konfigurace phishingových kampaní, nastavení uživatelských skupin, onboarding administrátorů i příprava prvních vzdělávacích scénářů. Zákazník získává připravené prostředí a metodickou podporu, zatímco každodenní plánování kampaní a práce s výsledky zůstává v kompetenci interního týmu.

Starter představuje ideální volbu pro organizace, které disponují vlastními bezpečnostními specialisty a chtějí mít celý vzdělávací program pod vlastní správou.

[COACH]

Plně řízený program bezpečnostního vzdělávání

Varianta Coach rozšiřuje možnosti platformy o dlouhodobou odbornou podporu týmu FreeDivision.

Vedle implementace a konfigurace zajišťujeme pravidelné plánování phishingových kampaní, průběžné vyhodnocování výsledků, doporučení pro další rozvoj bezpečnostního povědomí i manažerský reporting. Organizace získává kompletní program bezpečnostní osvěty bez nutnosti řešit každodenní administrativu nebo přípravu kampaní.

Součástí služby může být také integrace výsledků do prostředí FreeDivision.io Advanced, kde jsou informace o lidském riziku propojeny s dalšími bezpečnostními daty a podporují komplexní řízení bezpečnostních operací.

Typické scénáře využití

FreeDivision.io PhishingGym podporuje organizace ve všech fázích rozvoje bezpečnostního povědomí. Díky flexibilnímu modelu nasazení lze službu využít jako jednorázový projekt, pravidelný vzdělávací program i jako součást širší bezpečnostní strategie.

Pravidelné phishingové kampaně

Organizace potřebuje průběžně ověřovat odolnost zaměstnanců vůči aktuálním phishingovým technikám a současně sledovat, jak se bezpečnostní návyky vyvíjejí v čase.

FreeDivision.io PhishingGym umožňuje plánovat realistické kampaně během celého roku, vyhodnocovat jejich výsledky a systematicky zvyšovat odolnost uživatelů prostřednictvím navazujícího vzdělávání.

Vzdělávání po incidentu

Bezpečnostní incident nebo úspěšně zachycený phishing představuje vhodnou příležitost k okamžitému vzdělávání zaměstnanců.

Řešení umožňuje bezprostředně reagovat krátkým mikroškolením nebo cíleným vzdělávacím modulem zaměřeným na konkrétní typ útoku. Zaměstnanci si díky tomu snadněji osvojí správné postupy a jsou lépe připraveni na podobné situace v budoucnu.

Podpora regulatorních požadavků

Rostoucí počet organizací musí prokazovat, že bezpečnostní osvěta není jednorázovou aktivitou, ale dlouhodobě řízeným procesem.

FreeDivision.io PhishingGym poskytuje přehlednou evidenci školení, výsledků phishingových kampaní i trendů bezpečnostního povědomí. Tyto informace mohou sloužit jako podklady pro interní audit, regulatorní požadavky, NIS2, zákon o kybernetické bezpečnosti i interní bezpečnostní politiky.

Identifikace rizikových skupin

Ne všechny části organizace čelí stejným rizikům.

Díky detailnímu reportingu lze identifikovat týmy, pracovní role nebo lokality s vyšší mírou rizikového chování a přizpůsobit jim další vzdělávání. Organizace tak investuje čas i prostředky tam, kde mají největší dopad na celkovou úroveň bezpečnosti.

Přínosy pro organizaci

Hodnotou FreeDivision.io PhishingGym není samotné testování, ale dlouhodobé a měřitelné snižování lidského rizika.

Vyšší odolnost zaměstnanců

Pravidelné simulace a navazující vzdělávání pomáhají zaměstnancům lépe rozpoznávat phishing a sociální inženýrství, a tím snižovat pravděpodobnost úspěšného útoku.

Měřitelné snižování lidského rizika

Průběžná data ukazují vývoj bezpečnostního povědomí, rizikové skupiny i efektivitu vzdělávání, takže další opatření lze řídit podle skutečných výsledků.

Nižší zátěž interních týmů

Automatizace, připravené scénáře a možnost plně řízené služby zároveň snižují administrativní zátěž interních týmů a poskytují doložitelné podklady pro audit a compliance.

Proč FreeDivision

Úspěšná kybernetická bezpečnost nestojí pouze na moderních technologiích. Stejně důležití jsou lidé, správně nastavené procesy a schopnost dlouhodobě rozvíjet bezpečnostní kulturu celé organizace.

Proto stavíme všechna řešení platformy FreeDivision.io na třech vzájemně propojených pilířích.

Technologie

Využíváme moderní platformy pro phishingové simulace, mikroškolení a průběžné vyhodnocování bezpečnostního povědomí. Řešení pravidelně reflektuje aktuální trendy v oblasti phishingu, sociálního inženýrství i dalších útoků zaměřených na lidský faktor.

Naším cílem není pouze testovat zaměstnance, ale vytvářet prostředí, které podporuje dlouhodobé budování bezpečnostních návyků a poskytuje organizaci měřitelný přehled o vývoji lidského rizika.

Procesy

Bezpečnostní osvěta přináší dlouhodobé výsledky pouze tehdy, pokud je součástí pravidelného a systematického procesu.

FreeDivision.io PhishingGym propojuje plánování kampaní, vzdělávání, vyhodnocování výsledků i reporting do jednoho opakovatelného modelu. Organizace tak získává přehledný a dlouhodobě udržitelný program, který podporuje rozvoj bezpečnostní kultury a současně usnadňuje plnění interních i regulatorních požadavků.

Experti

Za úspěšným vzdělávacím programem nestojí pouze technologie, ale především zkušenosti odborníků, kteří rozumí současným hrozbám i fungování organizací.

Specialisté FreeDivision pomáhají navrhovat phishingové kampaně, interpretovat výsledky, doporučovat vhodné vzdělávací aktivity a plánovat dlouhodobý rozvoj bezpečnostního povědomí. Díky zkušenostem z implementace bezpečnostních projektů v různých typech organizací dokážeme přizpůsobit program konkrétním potřebám zákazníka.

Naším cílem není zaměstnance zkoušet nebo sankcionovat. Pomáháme organizacím vytvářet prostředí, ve kterém se lidé učí rozpoznávat rizika, správně reagovat na podezřelé situace a aktivně přispívat k ochraně firemních informací.

FreeDivision.io jako platforma pro komplexní kybernetickou bezpečnost

FreeDivision.io PhishingGym je součástí platformy FreeDivision.io, která propojuje technologie, odborné služby a řízení bezpečnosti do jednoho ekosystému.

Podle potřeb organizace jej lze rozšířit například o ochranu endpointů, řízení bezpečnostních operací, skenování a řízení zranitelností, ochranu dat, správu identit a přístupů, řízení rizik nebo služby Threat Intelligence.

Co nejlépe doplňuje FreeDivision.io PhishingGym

Ochrana koncových zařízení

FreeDivision.io Essential zajišťuje ochranu pracovních stanic, notebooků, serverů a dalších endpointů prostřednictvím moderních technologií EDR/XDR. Pomáhá včas detekovat hrozby, reagovat na incidenty a minimalizovat jejich dopad na provoz organizace.

Řízení bezpečnostních operací

FreeDivision.io Advanced poskytuje centralizované prostředí pro monitoring, korelaci bezpečnostních událostí, automatizaci reakcí a řízení bezpečnostních operací. Organizace získává jednotný pohled na stav své bezpečnostní architektury a efektivnější správu bezpečnostních procesů.

Odborné služby

FreeDivision.io Services rozšiřují technologickou platformu o zkušenosti specialistů FreeDivision. Zákazníci mohou využít podporu při návrhu, implementaci, provozu i dlouhodobém rozvoji bezpečnostního prostředí podle svých potřeb a interních kapacit.

Výsledky z **FreeDivision.io PhishingGym** lze integrovat do prostředí **FreeDivision.io Advanced**, kde se stávají součástí celkového pohledu na bezpečnostní stav organizace. Díky tomu lze lidské riziko vyhodnocovat společně s technickými bezpečnostními událostmi a získat komplexnější obraz o skutečné úrovni kybernetické odolnosti.

For Safety Reasons. Be Best. Not First.

Závěr

Lidský faktor zůstává důležitou součástí kybernetické odolnosti organizace. FreeDivision.io PhishingGym proto mění bezpečnostní osvětu z jednorázové povinnosti na pravidelný a měřitelný proces.
Díky kombinaci simulací, cíleného vzdělávání a průběžného vyhodnocování získává organizace možnost dlouhodobě snižovat lidské riziko a řídit rozvoj bezpečnostního povědomí na základě skutečných dat.
Ve spojení s dalšími řešeními FreeDivision.io představuje PhishingGym přirozenou součást bezpečnostní architektury, která vedle technologií systematicky rozvíjí i lidský faktor.

Připraveni posílit lidský článek vaší bezpečnosti?

Společně navrhneme program bezpečnostní osvěty odpovídající velikosti vaší organizace, jejím rizikům i regulatorním požadavkům. FreeDivision.io PhishingGym přináší vzdělávání, které je krátké, pravidelné, měřitelné a má reálný dopad na bezpečnostní návyky zaměstnanců.

ADRESA

FreeDivision s.r.o.
Rektorská 50/52
108 00 Praha 10 – Malešice
Česká republika

KONTAKT

sales@freedivision.com
+420 220 972 426

www.freedivision.io