Co-funded by the European Union

Online hrozby pro osoby starší 55 let – glosář

Co-funded by the
European Union

Phishing (podvodné e-maily, SMS, odkazy, hlasové hovory).

Phishing je typ kybernetického útoku, při kterém zločinci rozesílají falešné e-maily, textové zprávy, telefonní hovory nebo odkazy a vydávají se za někoho, komu důvěřujete, například za banku nebo přítele. Jejich cílem je oklamat vás a přimět vás, abyste poskytli důležité osobní údaje, jako jsou hesla, čísla kreditních karet nebo údaje o bankovním účtu. Tyto falešné zprávy často vypadají velmi reálně a snaží se vás přimět k rychlé akci tím, že ve vás vyvolají pocit naléhavosti nebo strachu. Útočníci vám chtějí ukrást peníze nebo identitu tím, že vás oklamou a přimějí vás kliknout na nebezpečné odkazy nebo sdílet citlivá data. Abyste zůstali v bezpečí, vždy si dvakrát ověřte, kdo zprávu odeslal, neklikejte na podezřelé odkazy a nikdy nesdílejte osobní údaje, pokud si nejste naprosto jisti, že jsou bezpečné.

Co-funded by the
European Union

Deepfake útoky (falešný zvuk/video, vydávání se za rodinu)

Útoky typu deepfake zahrnují vytváření falešných zvukových nebo obrazových nahrávek pomocí umělé inteligence, které vypadají a zní velmi realisticky. Při těchto útocích zločinci napodobují hlas nebo obličej někoho známého, často člena rodiny, aby lidi oklamali a přiměli je věřit, že mluví s milovanou osobou. Podvodník může například použít technologii deepfake k uskutečnění telefonního hovoru, který zní přesně jako hovor vnoučete, které naléhavě žádá o peníze. Tyto falešné nahrávky jsou velmi přesvědčivé a dokáží oklamat i opatrné lidi. Útoky typu deepfake jsou nebezpečné, protože zneužívají důvěru a emoce, takže je těžké si podvod uvědomit, dokud není příliš pozdě. Abyste se ochránili, vždy si před provedením jakýchkoli kroků ověřte neobvyklé požadavky tím, že danou osobu kontaktujete přímo prostřednictvím různých komunikačních kanálů.

Co-funded by the
European Union

Falešné internetové obchody a podvody (padělané webové stránky)

Falešné internetové obchody a podvody jsou podvodné webové stránky, které vypadají jako legitimní obchody, ale ve skutečnosti jsou vytvořeny tak, aby lidi oklamaly a přiměly k nákupu produktů, které neexistují nebo jsou nekvalitní. Tyto falešné obchody často kopírují loga, popisy produktů a fotografie skutečných společností, aby vypadaly přesvědčivě. Podvodníci tyto stránky používají k tomu, aby ukradli peníze a osobní údaje nic netušícím zákazníkům. Lákají kupující sliby velmi nízkých cen nebo speciálních nabídek, které se zdají být příliš dobré na to, aby byly pravdivé.

Tyto webové stránky mohou mít podivné webové adresy, obsahovat pravopisné chyby nebo postrádat správné kontaktní údaje. Poté, co zákazníci zaplatí, často svou objednávku nikdy neobdrží nebo dostanou padělané zboží. Abyste se chránili, nakupujte vždy v důvěryhodných obchodech, prostudujte si recenze na webových stránkách, vyhněte se nabídkám, které se zdají nerealisticky levné, a nikdy nesdílejte platební informace na podezřelých stránkách. Pokud se vám něco zdá divné, je lepší si to před nákupem dvakrát ověřit.

Co-funded by the
European Union

Emoční manipulace a sociální inženýrství (zastrašovací taktiky).

Emoční manipulace a sociální inženýrství zahrnují podvádění lidí hraním na jejich city, aby se chovali způsobem, jakým by se normálně nechovali. Kyberzločinci používají taktiky, jako jsou strašidelné historky, naléhavost, falešná autorita nebo laskavost, k vytvoření pocitu strachu, důvěry nebo povinnosti. Mohou se například vydávat za bankovního úředníka, který vás varuje před problémem s vaším účtem a naléhá na vás, abyste jednali rychle, abyste bez přemýšlení poskytli citlivé informace. Tyto taktiky zneužívají přirozené lidské reakce – strach, důvěru, zvědavost nebo ochotu pomoci – a je tak těžké jim odolat. Nejlepší obranou je uvědomění si: rozpoznání těchto emocionálních triků a zastavení se, abyste si ověřili, kdo se o informace skutečně ptá, než odpovíte.

Co-funded by the
European Union

Krádež identity (s využitím ukradených osobních údajů)

Krádež identity znamená, že někdo bez vašeho svolení ukradne vaše osobní údaje a použije je k tomu, aby se za vás vydával. Může použít vaše jméno, číslo sociálního zabezpečení, údaje o bankovním účtu nebo jiné údaje k otevření účtů, sjednání půjček nebo k nákupům vaším jménem. To může způsobit velké finanční problémy a poškodit vaši pověst.

Co-funded by the
European Union

Podvod „na vnoučeti“ (podvodníci předstírající, že jsou členy rodiny v nouzi)

Podvod „na vnoučeti“, známý také jako „podvod s prarodiči“, je běžná metoda používaná zločinci, kteří se vydávají za člena rodiny – obvykle vnouče nebo dítě – v nouzi. Obvykle se to děje telefonicky, kdy podvodník zavolá starší osobě a tvrdí, že je ve vážných potížích, například že měla nehodu, byla zatčena nebo potřebuje naléhavou finanční pomoc. Volající často požádá o rychlé zaslání peněz a trvá na tom, aby oběť to udržela v tajnosti, například slovy: „Neříkej to mámě, bude se bát.“

Tento podvod hraje na emoce, jako je láska a zájem o členy rodiny, a v dané osobě vyvolává touhu okamžitě pomoci, aniž by se musela zastavit. Podvodníci stále častěji využívají technologie, jako je umělá inteligence, k napodobení hlasu skutečného vnoučete, díky čemuž hovor zní velmi přesvědčivě.

Co-funded by the
European Union

Falešné žádosti o „pomoc“ přes WhatsApp nebo Messenger

Falešné žádosti o „pomoc“ přes WhatsApp nebo Messenger jsou podvody, kdy se někdo vydává za přítele nebo člena rodiny v naléhavých nouzích a žádá o peníze nebo osobní údaje. Tyto zprávy často přicházejí nečekaně od neznámých nebo maskovaných kontaktů. Podvodník může tvrdit, že ztratil telefon, že se mu zablokoval účet nebo že potřebuje naléhavou finanční pomoc. Snaží se vytvořit pocit naléhavosti a důvěry, aby oběti přiměl k rychlé reakci, aniž by si ověřoval, zda je to pravda.

Co-funded by the
European Union

Romantické podvody a podvody založené na vztazích budovaných online

Romantické podvody jsou typem podvodu, kdy zločinci vytvářejí falešné online profily a předstírají romantický zájem o někoho. Postupem času si budují důvěru a emocionální pouto, čímž oběť přesvědčí, že je ve skutečném vztahu. Jakmile si podvodníci získají důvěru, vymýšlejí si nouzové situace nebo naléhavé finanční potřeby – jako jsou lékařské výdaje nebo cestovní náklady – a po oběti žádají o peníze nebo dárky.

Tito podvodníci jsou velmi zruční v předstírání starostlivosti a důvěryhodnosti a často se vyhýbají osobním schůzkám nebo videohovorům podáním výmluv. Zneužívají osamělosti a emocionální zranitelnosti, což zvyšuje pravděpodobnost, že jim oběti dají peníze.

Co-funded by the
European Union

Investiční podvod (falešné reklamy s celebritami).

Investiční podvod zahrnující falešné reklamy celebrit je typ podvodu, kdy zločinci používají obrázky, videa nebo jména slavných osobností, aby investiční příležitost vypadala legitimně a důvěryhodně. Někdy tyto reklamy obsahují falešná videa, na kterých celebrity podporují investici, nebo se vydávají za novinové články spojující celebrity s finančním úspěchem na určitých platformách.

Podvodníci klamou lidi, aby věřili, že mohou dosáhnout rychlých a velkých zisků, často v kryptoměnách nebo obchodování s devizami. Lákají oběti k vytvoření účtů, vložení peněz a poté požadují další prostředky na zaplacení falešných poplatků nebo daní. Důvěru lze získat předčasným výběrem, ale když se oběti pokusí vybrat své peníze, jsou zablokovány a požadovány vysoké dodatečné platby.

Co-funded by the
European Union

Malware a ransomware (infikované soubory, přílohy)

Malware je škodlivý software, který může infikovat váš počítač nebo telefon a způsobit škodu, například krádež osobních údajů, poškození souborů nebo převzetí kontroly nad vaším zařízením. Ransomware je speciální typ malwaru, který uzamyká nebo šifruje vaše soubory a znepřístupňuje je, dokud útočníkovi nezaplatíte výkupné – obvykle v kryptoměně. Ransomware se do vašeho zařízení může dostat prostřednictvím infikovaných e-mailových příloh, škodlivých webových stránek nebo nebezpečných stahovaných souborů.

Jakmile je ransomware infikován, znemožní vám používat důležité soubory a někdy požaduje peníze za obnovení přístupu. Zaplacení výkupného nezaručuje, že vaše data budou uvolněna, a povzbuzuje zločince k pokračování v těchto útocích.

Co-funded by the
European Union

Neověřené aplikace a stahování nebezpečného softwaru

Neověřené aplikace a nebezpečné stahování softwaru jsou kybernetické hrozby, kdy si lidé stahují a instalují aplikace nebo soubory z neznámých nebo nespolehlivých zdrojů. Tyto aplikace nebo stahování mohou obsahovat skrytý malware, viry nebo spyware, které mohou poškodit vaše zařízení, ukrást osobní údaje nebo poskytnout hackerům neoprávněný přístup.

Protože tyto aplikace nejsou kontrolovány ani schvalovány důvěryhodnými platformami, mohou narušovat zabezpečení vašeho zařízení, způsobovat pády nebo vás vystavovat podvodům. Falešné aplikace mohou vypadat jako skutečné, ale po instalaci mohou shromažďovat vaše data nebo šířit škodlivý software.

Co-funded by the
European Union

Sdílení citlivých údajů s cizími lidmi (fotografie, informace).

Sdílení citlivých dat s cizími lidmi, jako jsou fotografie nebo osobní údaje, je kybernetická hrozba, kdy lidé online sdělují soukromé údaje neznámým nebo nedůvěryhodným lidem. Může se to zdát neškodné, jako sdílení fotografie, ale tyto údaje mohou být zneužity k odcizení vaší identity, spáchání podvodu nebo poškození vaší pověsti.

Fotografie mohou odhalit váš domov, polohu nebo osobní zvyky, aniž byste si to uvědomovali. Cizí lidé mohou tyto informace použít k tomu, aby vás oklamali nebo se na vás zaměřili v podvodných akcích. Abyste zůstali v bezpečí, sdílejte osobní údaje a fotografie pouze s lidmi, kterým důvěřujete, pečlivě si rozmyslete, než je zveřejníte online, a upravte nastavení soukromí tak, abyste omezili, kdo může vaše informace vidět.

Co-funded by the
European Union

Úniky dat z používání zastaralých zařízení nebo softwaru

Používání zastaralých zařízení nebo softwaru představuje kybernetickou hrozbu, protože staré verze často neobsahují nejnovější bezpečnostní aktualizace. Tyto chybějící aktualizace vytvářejí slabiny, které mohou hackeři snadno zneužít k přístupu k vašim osobním údajům nebo k ovládání vašeho zařízení. To může vést k úniku dat, krádeži nebo napadení malwarem.

Zastaralý software také zpomaluje vaše zařízení a může přestat fungovat s novějšími programy, což vám ztěžuje každodenní činnosti. Abyste se chránili, je důležité pravidelně aktualizovat zařízení a důležitý software nejnovějšími záplatami a bezpečnostními opravami. Tím se odstraní bezpečnostní mezery, zajistí se bezpečnější data a zajistí se bezproblémový chod zařízení.

Co-funded by the
European Union

Masové personalizované útoky s využitím umělé inteligence, zaměřené na uživatelské profily

Masově personalizované útoky s využitím umělé inteligence jsou kybernetické hrozby, kdy útočníci využívají umělou inteligenci k vytváření vysoce personalizovaných a přesvědčivých zpráv zaměřených na jednotlivce, na základě jejich osobních údajů. Umělá inteligence analyzuje informace ze sociálních médií, e-mailů a veřejných zdrojů a vytváří zprávy, které cíli působí velmi povědomě a důvěryhodně.

Tyto útoky mohou zahrnovat personalizované phishingové e-maily nebo zprávy, které zmiňují jméno oběti, její zaměstnání, nedávné aktivity či zájmy. Cílem je oklamat lidi, aby klikli na škodlivé odkazy, odhalili hesla nebo převedli peníze. Protože se umělá inteligence neustále učí a přizpůsobuje, stávají se tyto útoky efektivnějšími a hůře odhalitelnými.

Co-funded by the
European Union

Zdravotní dezinformace nebo nebezpečné lékařské rady z nástrojů umělé inteligence

Zdravotní dezinformace nebo nebezpečné lékařské rady z nástrojů umělé inteligence představují kybernetickou hrozbu, kdy umělá inteligence generuje nesprávné, zavádějící nebo škodlivé zdravotní informace. Lidé mohou důvěřovat chatbotům s umělou inteligencí nebo online nástrojům, pokud jde o lékařské rady, ale tyto systémy někdy vytvářejí nesprávné diagnózy, navrhují nebezpečnou léčbu nebo šíří nepravdivá tvrzení o nemocech.

Tato dezinformace může vést k tomu, že lidé odkládají poskytnutí řádné lékařské péče, používají neúčinné léky nebo se dopouštějí škodlivých činů. Obsah generovaný umělou inteligencí může znít velmi profesionálně a přesvědčivě, takže je obtížné určit, zda je rada spolehlivá.

Co-funded by the
European Union

Podvody zneužívající digitální vyloučení v občanských a bankovních službách

Podvody zneužívající digitální vyloučení v občanských a bankovních službách jsou hrozby zaměřené na osoby, které mají omezený přístup k digitálním technologiím nebo o nich mají malou znalost. Tyto podvody zneužívají lidi, kteří mají potíže s používáním online vládních nebo bankovních služeb, někdy proto, že jim chybí zařízení, přístup k internetu, digitální dovednosti nebo sebevědomí.

Zločinci tyto osoby podvádějí tím, že nabízejí falešnou pomoc s online procesy nebo zasílají podvodné zprávy napodobující oficiální instituce v naději, že oběti sdílejí citlivé údaje nebo pošlou peníze. Protože tito lidé mají méně zdrojů nebo podpory k rozpoznání podvodů, jsou zranitelnější.

Co-funded by the
European Union

Nedostatek postupů vícefaktorového ověřování (zjednodušená hesla, opakované použití)

Absence vícefaktorového ověřování (MFA) znamená používání pouze hesla – často jednoduchého nebo opakovaného na mnoha webech – k ochraně online účtů. To je riskantní, protože pokud někdo vaše heslo ukradne nebo uhádne, může se snadno dostat k vašim účtům.

Vícefaktorové ověřování přidává další vrstvu zabezpečení tím, že vyžaduje dvě nebo více forem ověření. Například po zadání hesla můžete zadat kód odeslaný na váš telefon nebo použít skenování otisků prstů. To hackerům výrazně ztěžuje přístup k vašemu účtu, i když znají vaše heslo.

Co-funded by the
European Union

Ztráta přístupu ke klíčovým službám v důsledku technologických změn (přístup pouze přes aplikaci, omezené alternativy)

Ke ztrátě přístupu ke klíčovým službám v důsledku technologických změn dochází, když důležité veřejné nebo bankovní služby přecházejí do čistě digitálních formátů, jako jsou aplikace nebo online portály, bez snadných alternativ pro lidi, kteří se k jejich používání necítí dobře nebo nejsou vybaveni. To znamená, že lidé, kteří nemají chytré telefony, počítače nebo digitální dovednosti, mohou mít potíže s přístupem k základním službám, jako jsou návštěvy zdravotní péče, důchodové dávky nebo bankovní transakce, nebo jim tento přístup vůbec nemohou umožnit.

Tento digitální posun může vyloučit mnoho lidí, zejména starší dospělé nebo osoby s omezenými zdroji, a učinit je tak závislými na ostatních nebo neschopnými plnit důležité úkoly.

Co-funded by the
European Union

Automatizovaná manipulace sociálních médií, produkující dezinformace a stres

Automatizovaná manipulace se sociálními sítěmi je kybernetická hrozba, kdy počítačové programy, nazývané boti, a umělá inteligence ovládají obsah, který vidíte na svých stránkách sociálních sítí. Tyto systémy analyzují, co se vám líbí, co sdílíte nebo co komentujete, a poté vám zobrazují podobné příspěvky, abyste si udrželi zájem.

Tohoto přístupu bohužel lze využít k šíření dezinformací, falešných zpráv nebo extrémního obsahu, který vyvolává stres, strach nebo hněv. Boti mohou uměle zvyšovat popularitu takových příspěvků lajkováním, sdílením nebo komentováním, čímž vytvářejí dojem, že s nimi mnoho lidí souhlasí.