TeleGrow
Enhancing the Teleworking Digital Skills for the Middle aged employees

Moduły szkoleniowe How to TeleGrow: Ostateczne szkolenie z zakresu telepracy dla dostawców VET

CWEP

Moduł 6 - Podstawy bezpieczeństwa w sieci

27/6/2022

Erasmus+

Projekt finansowany przez: **Call 2020 Round 1 KA2 - Cooperation for innovation and exchange of good practices/ KA226 - Partnerships for Digital Education Readiness.**

Indeks

1. Wprowadzenie do tematu

W tych trudnych czasach wszyscy ludzie próbują dostosować się do nowej pracy w domu bez obowiązkowej wiedzy o ilości ryzyka i zagrożeń nie tylko dla osób w wieku 50+, do których skierowany jest projekt. TeleGrow jest adresowany do pracowników w każdym wieku. Raport Komisji Europejskiej z 2020 roku podaje, że od czasu pandemii COVID-19 około 40 procent pracowników w UE rozpoczęło pracę zdalną, co stanowi prawie 8-krotny wzrost w porównaniu z rokiem poprzedzającym jej rozpoczęcie. Ten szybki wzrost telepracy utrudnia firmom wdrożenie nowych i silnych zabezpieczeń, co otwiera okno dla różnych złośliwych praktyk. Przy wzroście aktywności cyberprzestępczej od początku pandemii o ponad 600proc, łatwo dojść do wniosku, że osoby w wieku 50+, które miały niewielkie lub żadne doświadczenie z telepracą, są szczególnie narażone na niebezpieczeństwa, jakie może ona przynieść. Niebezpieczeństwa te obejmują takie rzeczy jak kradzież tożsamości, naruszenie danych, złośliwe oprogramowanie (malware) i wirusy, oszustwa bankowe i wiele innych zagrożeń, na które osoby starsze mogą nie być dobrze przygotowane.

Niniejszy moduł został zaprojektowany jako krótkie wprowadzenie do tematu bezpieczeństwa w sieci. Będzie zawierał opisy najczęstszych zagrożeń związanych z telepracą i ogólnym korzystaniem z Internetu, z którymi mogą spotkać się grupy docelowe projektu TeleGrow. Ta część modułu pomoże zrozumieć czym jest spam i phishing, jak je rozpoznać i jakie zagrożenia mogą nieść. Inne powszechne praktyki, takie jak hakerstwo, ransomware czy kradzież tożsamości, również zostaną opisane i wyjaśnione.

Moduł wyjaśni również, jakie środki powinny być podjęte w celu zabezpieczenia prywatnego połączenia internetowego i zapozna uczącego się z Ogólnym Rozporządzeniem o Ochronie Danych. Wreszcie, ten moduł projektu TeleGrow będzie zawierał również krótki zestaw ćwiczeń dla swoich uczniów, aby sprawdzić ich wiedzę nabytą w tym module.

2. Cele dydaktyczne

Po ukończeniu tego modułu uczący się będzie:

- uczyć się o spamie i phishingu oraz o tym, jak je rozpoznać
- zrozumieć, czym jest hakerstwo, jak działa ransomware i jak chronić się przed kradzieżą tożsamości i związanymi z nią konsekwencjami
- wiedzą, jakie środki należy podjąć, aby zabezpieczyć swoje połączenie internetowe i jaka jest różnica między słabym a silnym hasłem.
- zdobycie wiedzy na temat ogólnego rozporządzenia o ochronie danych osobowych oraz sposobów ochrony danych osobowych
- być w stanie stworzyć bezpieczne środowisko pracy w domu z wykorzystaniem praktycznego działania na koniec modułu

3. Treści nauczania

Rozdział 1 - Spam i Phishing

Słowo "spam" odnosi się do wszelkich niechcianych wiadomości cyfrowych otrzymywanych przez ludzi, które zostały wysłane do dużej grupy odbiorców. Proces ten jest najczęściej wykonywany przez rzeczy zwane "spambotami", które są zautomatyzowanymi programami używanymi do wysyłania wiadomości spamowych na konta e-mail, portale społecznościowe lub fora. Mimo że spam może wydawać się stosunkowo nowym problemem, jego historia sięga 1978 roku, kiedy to Gary Thuerk chciał promować swój produkt poprzez wysyłanie niechcianych wiadomości e-mail do tysięcy osób, co rzekomo wygenerowało około 12 milionów dolarów przychodu.

Dzisiejsze wykorzystanie wiadomości spamowych pozostaje w większości przypadków takie samo, ponieważ są one wykorzystywane do generowania zysku poprzez promowanie czegoś. Generalnie, reklamowane przez niego produkty są wątpliwej jakości, a tematy, które najczęściej reklamują wiadomości spamowe to:

- farmaceutyki
- treści dla dorosłych
- usługi finansowe
- gry hazardowe online
- kryptowaluty

Źródło: freepik.com

W 2020 roku około 50% wszystkich otrzymanych wiadomości e-mail stanowiło spam. Osoby tworzące i wysyłające wiadomości spamowe żerują na niedoświadczonych użytkownikach Internetu, a otwieranie takich e-maili może mieć bardzo nieprzyjemne konsekwencje, takie jak udostępnianie prywatnych informacji nieupoważnionym osobom lub trafienie na listy mailingowe różnych sprzedawców, co doprowadzi do jeszcze większej ilości niechcianych e-maili piętrzących się w czyjejś skrzynce pocztowej. Mimo że liczby mogą wydawać się przytłaczające, ludzie rzadko widzą obecnie wiadomości spamowe w swoich skrzynkach pocztowych. Jest to spowodowane szybkim rozwojem w dziedzinie filtrowania spamu. Statystyki ujawnione przez Google w kwietniu 2020 roku pokazały, że udało im się z powodzeniem zablokować i przefiltrować 99,9% wiadomości spamowych. Oznacza to, że dzisiejsi internauci, wraz z osobami w wieku 50+, są znacznie bezpieczniejsi od otrzymywania tego typu wiadomości. Nie oznacza to jednak, że filtrowanie działa bez zarzutu; nadal zdarzają się wiadomości spamowe, które przedostają się do sieci, a żeby móc je samodzielnie odfiltrować, internauci powinni wiedzieć, jakiego typu wiadomości powinni unikać. Niektóre z najczęstszych typów spamu to:

- Fałszowanie wiadomości e-mail

  Tego typu wiadomości próbują naśladować nadawcę, podrabiając ten sam dokładny e-mail jak oni i oszukując odbiorcę, że e-mail pochodzi od osoby lub strony internetowej, której można zaufać. Często prosi kogoś o podjęcie jakiegoś działania, które może być prośbą o zapłatę zaległej faktury, zatwierdzenie/odblokowanie konta, lub weryfikację zakupu, i dostarcza link, który po kliknięciu może być wykorzystany do kradzieży danych osobowych odbiorcy. Na szczęście wielu dostawców poczty elektronicznej ostrzega wcześniej użytkownika o ryzyku bycia "spoofed".

- Oszustwa polegające na wpłacaniu zaliczek

  Czasami określane jako "oszustwo nigeryjskiego księcia", jedną z idei stojących za tym jest to, że nadawca obiecuje dużą sumę pieniędzy, ale tylko wtedy, gdy odbiorca zapewni małą pożyczkę z góry. Ta pożyczka jest zwykle powiedział, że jest

wymagana dla jakiegoś rodzaju sprawy prawnej, która będzie odblokować większą sumę. Inny rodzaj oszustwa typu opłata zaliczkowa działa w podobny sposób, ale w tym przypadku nadawca udaje bliskiego przyjaciela lub członka rodziny odbiorcy, który potrzebuje pieniędzy z powodu jakiegoś nagłego wypadku.

- Reklamy i spam związany ze złośliwym oprogramowaniem

Spam reklamowy to po prostu niechciana wiadomość oferująca jakiś rodzaj produkt. Chociaż oferty te mogą być czasami prawdziwe, w wielu przypadkach produkt albo nie istnieje, albo nie będzie działał. Spam zawierający złośliwe oprogramowanie to rodzaj wiadomości, która zawiera różnego rodzaju złośliwe treści ukryte za odsyłaczami lub załącznikami znajdującymi się w wiadomości. Gdy osoba pobierze i otworzy załączony plik lub pobrany za pośrednictwem łącza, złośliwe skrypty zostaną uruchomione i zainfekują komputer różnymi rodzajami niebezpiecznego malware.

Źródło: freepik.com

- Phising

Podobnym do email spoofingu, ale bardziej złożonym cyberprzestępstwem jest phishing. Ta złośliwa praktyka jest stosowana w kontekście oszustwa, szpiegostwa lub w celu przeprowadzenia cyberataków skierowanych na różne organizacje. Polega ona na fałszowaniu wiadomości e-mail lub rozmów telefonicznych i podawaniu się za pochodzące z legalnego źródła w celu przekonania osób do ujawnienia swoich danych

osobowych lub finansowych, często bez konkretnego celu. Wiadomości Spear phishing są również wysyłane ze sfałszowanych e-maili wyglądających na godne zaufania, ale w tym przypadku cyberprzestępca zbiera informacje o ofierze z różnych źródeł, takich jak publiczne posty w mediach społecznościowych, strony, na których zarejestrowany jest e-mail ofiary, profile znajomych ofiary w mediach społecznościowych lub informacje o pracownikach na stronie internetowej firmy.

Haker może wtedy zebrać wszystkie informacje o tej osobie i przygotować spersonalizowaną wiadomość, której ofiarą może paść odbiorca. Wiadomości te często zawierają złośliwe linki, ale mogą być również wykorzystane do stworzenia połączenia między przestępcą a ofiarą w celu zdobycia zaufania i kradzieży poufnych informacji. Czasami ataki typu wyłudzanie informacji są wymierzone w osoby zajmujące wysokie stanowiska kierownicze w firmie, aby podstępem zmusić je do ujawnienia swoich danych osobowych lub cennych danych firmowych, które później mogą zostać wykorzystane do złych celów. Aby być mniej podatnym na próby phishingu, użytkownicy Internetu powinni zwracać szczególną uwagę na otwieranie stron internetowych i unikać ich:

- E-maile o wygraniu dużej nagrody
- Fałszywe strony internetowe ściśle przypominające oryginalne
- Groźby dotyczące dezaktywacji konta lub utraty dostępu do niego
- Wiadomości o fałszywej infekcji złośliwym oprogramowaniem
- Maile tematyczne COVID-19
- Fałszywi krewni proszący o pieniądze
- Słaba gramatyka i błędnie napisane słowa w rzekomo formalnych e-mailach

Mimo, że filtry złośliwych treści dostarczane przez większość dostawców poczty elektronicznej oferują silną ochronę przed spamem i phishingiem, ludzie powinni pamiętać, że nie są one pozbawione wad i istnieją pewne środki zaradcze, które mogą podjąć, aby jeszcze bardziej zmniejszyć szanse na kradzież ich danych osobowych. Aby to osiągnąć, ludzie powinni zawsze kopiować i wklejać treść podejrzanej wiadomości do wyszukiwarki (np. Google), ponieważ istnieje szansa, że została ona wcześniej

zgłoszona jako próba phishingu. Inną dobrą praktyką jest skontaktowanie się z firmą, która rzekomo wysłała podejrzaną wiadomość, bez klikania linków lub załączników, które znajdowały się wewnątrz niej. Dobrym pomysłem jest również zainstalowanie na komputerze filtrów antyspamowych i pasków antyphishingowych, ponieważ narzędzia te mogą same ochronić użytkownika przed takimi wiadomościami. W środowisku pracy pracownicy powinni starać się potwierdzać słownie wszelkie prośby wysyłane do nich za pośrednictwem poczty elektronicznej oraz regularnie zmieniać swoje hasła.

Rozdział 2 - Hacking, Ransomware, kradzież tożsamości

Ze względu na obserwowany ostatnio wzrost telepracy oraz konieczność pozostania w domu i załatwiania wielu spraw online z powodu pandemii COVID-19, na świecie obserwuje się również ogromny wzrost cyberprzestępczości. Można je zdefiniować jako wszelkie nielegalne działania wykonywane przy użyciu komputera i są często związane z osobami zwanymi "hakerami" lub "cyberprzestępcami", których można podzielić na wiele różnych kategorii w zależności od tego, co chcą osiągnąć i jak bardzo są wykwalifikowani.

Źródło: freepik.com

Hacking to proces identyfikowania luk w zabezpieczeniach systemu komputerowego lub sieci w celu uzyskania dostępu do danych osobowych lub biznesowych. Wykorzystanie algorytmu rozszyfrowywania haseł w celu uzyskania dostępu do systemu komputerowego jest przykładem hakowania komputerowego. Chociaż często jest to uważane za złośliwą praktykę, czasami jest legalne i używane w dobrych intencjach, głównie w celu poprawy bezpieczeństwa online i zabezpieczenia cennych danych wewnątrz określonej organizacji. Taka praktyka nazywana jest "etycznym hackingiem". Zwykły hacking obejmuje szerokie spektrum złośliwych praktyk, począwszy od spowalniania komputerów innych osób, poprzez kradzież informacji o kartach kredytowych, aż po zastraszanie na dużą skalę i żądania okupu. Jak wspomniano w rozdziale 1, hakerzy mogą uzyskać dostęp do urządzeń innych osób poprzez próby phishingu i złośliwe oprogramowanie zawarte w podejrzanych wiadomościach spamowych, ale nie są to jedyne metody, których używają. Popularną techniką hakerską, na którą wiele osób może być podatnych, jest stworzenie fałszywego punktu dostępu do sieci Wi-Fi w miejscu publicznym, który po połączeniu przekieruje ofiarę na stronę internetową, która może wykraść ich dane osobowe. Aby temu zapobiec, ludzie powinni unikać korzystania z publicznych sieci Wi-Fi i zawsze zachować ostrożność podczas korzystania ze swoich urządzeń w miejscach takich jak restauracje, lotniska, centra handlowe czy parki.

Inną formą złośliwego oprogramowania, która może być bardzo niebezpieczna dla osób w wieku 50+, które dopiero zaczynają telepracę, jest **ransomware.** Okazało się ono bardzo niebezpieczne, ponieważ jest nie tylko jednym z najbardziej niepokojących problemów bezpieczeństwa internetowego w dzisiejszych czasach, ale jest również bardzo powszechne. To złośliwe oprogramowanie szyfruje pliki i dokumenty na wszystkim, od pojedynczego komputera po całą sieć, w tym serwery. Po ataku ransomware ofiara otrzymuje instrukcje dotyczące zapłacenia okupu w celu odblokowania plików; w przeciwnym razie cenne dane zostaną upublicznione lub sprzedane innym cyberprzestępcom, stąd nazwa "ransomware". Ten i inne malwares, są najczęściej rozprzestrzeniane poprzez załączniki w spamie phishingowym, dlatego tak ważne jest, aby traktować wszelkie podejrzane e-maile z najwyższą ostrożnością.

Ataki typu ransomware są bardzo niebezpieczne, ponieważ w przypadku powodzenia mogą ujawnić cenne, prywatne informacje tysięcy pracowników, jeśli ich celem jest konkretna firma.

Źródło: freepik.com

Jedną z najszybciej rozwijających się form cyberprzestępczości jest kradzież tożsamości. Przestępca kradnie dane osobowe, takie jak dane uwierzytelniające, dane konta bankowego, daty urodzenia itp. w celu podszycia się pod ofiarę i wykorzystania tych informacji do uzyskania zysku pieniężnego i wyrządzenia dalszych szkód ludziom. Metody, których używają hakerzy, aby to zrobić, są podobne do innych cyberprzestępstw. Mogą zdobyć te cenne dane poprzez próby phishingu lub włamania do komputerów przy użyciu różnych złośliwych programów i fałszywych lub źle zabezpieczonych publicznych punktów dostępu Wi-Fi. Później mogą wykorzystać te dane do uzyskania pożyczek, zakupu różnych rzeczy, a nawet popełnienia przestępstw w imieniu ofiary. Dobrze jest regularnie sprawdzać raporty kredytowe i szukać wszelkich nieścisłości lub przelewów bankowych, które mogą wydawać się podejrzane. Suma brakujących pieniędzy nie musi być duża, bo złodziej może okradać tysiące osób jednocześnie. Ofiary kradzieży tożsamości powinny, tak szybko jak to możliwe, zgłosić to przestępstwo władzom, zamrozić swoje konta bankowe i otworzyć nowe. Jeśli jest to możliwe, ofiary powinny skontaktować się z bankami, firmami windykacyjnymi i innymi miejscami, o których wiedzą, że złodziej wykorzystał ich dane

osobowe. Ważne jest również, aby skontaktować się z krewnymi, pracodawcami i kolegami z aktualnie zatrudnionej firmy, ponieważ złodziej może być w posiadaniu również ich informacji.

Techniki stosowane przez hakerów w celu kradzieży lub wprowadzenia chaosu do życia ludzi stają się coraz bardziej wyrafinowane. Pamiętając o tym, ludzie muszą wiedzieć, jak się chronić, aby zminimalizować szanse bycia jedną z ofiar cyberprzestępstw. Istnieje jedno pewne przeciwdziałanie ochronne, które po wdrożeniu zmniejsza ryzyko związane z kontaktem z cyberprzestępcami.

Stwórz silne hasło. Jest to kluczowe dla zachowania bezpieczeństwa cennych danych. Dobre hasło nie jest oczywiste, ale jest łatwe do zapamiętania. Nie powinno być krótsze niż 12 znaków, ponieważ przy dzisiejszej technologii złamanie krótkich haseł zajmuje kilka sekund. Silne hasło powinno zawierać unikalne symbole, takie jak cyfry i małe lub duże litery, ponieważ doda to do niego dodatkową warstwę bezpieczeństwa. Ważne jest, aby było ono silne i trudne do zapomnienia. Popularną techniką tworzenia silnych haseł jest tworzenie akronimu z ulubionego cytatu lub frazy, która zapada w pamięć i dodanie do niej kilku symboli specjalnych. Inną dobrą praktyką jest korzystanie z menedżerów haseł. Programy te generują i przechowują hasła użytkownika na jednym, bezpiecznie zaszyfrowanym koncie. Ważną rzeczą jest również zachowanie poufności haseł i niewysyłanie ich nikomu za pośrednictwem poczty elektronicznej lub wiadomości tekstowych. Na podstawie zebranych danych, poniższy wykres pokazuje, jak trudno jest hakerowi złamać hasło, które może wydawać się skomplikowane dla jego użytkownika.

Z zebranych danych łatwo potwierdzić to, co zostało wcześniej stwierdzone. Hasło o długości 12 znaków powinno być minimum dla optymalnego bezpieczeństwa i nie musi być nawet naprawdę skomplikowane. Aby było ono nie do złamania przez co najmniej 300 lat, wystarczy hasło z małymi i wielkimi literami. Należy zauważyć, że nie **zaleca się podawania własnego nazwiska jako hasła,** ponieważ może ono zostać łatwo złamane, niezależnie od jego długości.

WYKRES ZŁOŻONOŚCI HASŁA

LICZBA ZNAKÓW	TYLKO CYFRY	MAŁE LITERY	MAŁE I DUŻE LITERY	CYFRY, MAŁE I DUŻE LITERY	SYMBOLE, CYFRY, MAŁE I DUŻE LITERY
6	Natychmiast	Natychmiast	Natychmiast	1 sekunda	5 sekund
7	Natychmiast	Natychmiast	25 sekund	1 minuta	6 minut
8	Natychmiast	5 minut	22 minuty	1 godzina	8 godzin
9	Natychmiast	2 minuty	19 hours	3 dni	3 tygodnie
10	Natychmiast	58 minut	1 miesiąc	7 miesięcy	5 lat
11	2 sekundy	1 dzień	5 lat	41 lat	400 lat
12	25 sekund	3 tygodnie	300 lat	2k lat	34k lat
13	4 minuty	1 rok	16k lat	100k lat	2m lat
14	41 minut	51 lat	800k lat	9m lat	200m lat

Dane zebrane na stronie: https://www.security.org/how-secure-is-my-password/

Rozdział 3 - Bezpieczne połączenie internetowe

Powszechnie wiadomo, że Internet jest niezawodnym, ale niebezpiecznym źródłem informacji i rozrywki. Ze względu na ilość złośliwego oprogramowania, szpiegów i hakerów, którzy tylko czekają na dobrą okazję do ataku, ważne jest, aby wiedzieć, jak się przed nimi bronić, ponieważ czasami dobre hasło nie wystarczy. Istnieje wiele sposobów, które mogą zwiększyć bezpieczeństwo połączenia internetowego, a wiele z nich nie wymaga zaawansowanej wiedzy technologicznej.

Na początek warto wdrożyć **dwuskładnikowe uwierzytelnianie** (2FA), gdy tylko jest to możliwe. Już samo to może zniechęcić większość hakerów do włamania się na czyjeś konto. Działa jako druga warstwa weryfikacji podczas logowania na konto, podczas gdy jedna to zazwyczaj hasło, druga to często unikalny klucz wysyłany na numer telefonu komórkowego użytkownika, który należy wprowadzić po zalogowaniu się za pomocą hasła. Jest to uważane za naprawdę silną metodę ochrony użytkowników

przed niebezpieczeństwem kradzieży ich haseł, ponieważ unikalność klucza znacznie utrudnia hakerowi włamanie się na konto.

Inną dobrą praktyką jest korzystanie z **wirtualnej sieci prywatnej (VPN)**. Za każdym razem, gdy ktoś łączy się z siecią, strumień danych jest wymieniany między użytkownikiem a serwerami. VPN tworzy bezpieczne połączenie pomiędzy tymi dwoma stronami poprzez szyfrowanie danych przed ich wysłaniem lub otrzymaniem przez użytkowników. VPN ukrywa adres IP użytkownika i jego lokalizację, więc cyberprzestępcy nie mogą już odkryć lokalizacji swoich potencjalnych ofiar, ponieważ dzięki VPN śledziliby je do lokalizacji serwera VPN, co znacznie utrudniłoby wgląd w ich dane. Jest to świetne narzędzie do zabezpieczenia połączenia podczas korzystania z publicznych sieci Wi-Fi w miejscach takich jak lotniska czy restauracje, które są łatwe do zhakowania.

Źródło: freepik.com

Aby skonfigurować ten rodzaj połączenia, konieczne jest znalezienie wiarygodnego dostawcy usług VPN i zapisanie się do niego. Na rynku jest kilku dostawców, którzy oferują swoje usługi za darmo, ale zaleca się nabycie płatnej subskrypcji, ponieważ oferuje ona więcej funkcji dla bezpieczniejszego połączenia. Po znalezieniu

preferowanego dostawcy VPN, użytkownik zostanie poproszony o pobranie niezbędnego oprogramowania. Musi być ono zawsze pobierane bezpośrednio ze strony internetowej dostawcy, ponieważ pobieranie z innego źródła może spowodować pobranie plików zawierających złośliwe oprogramowanie. Większość aplikacji VPN jest dostępna na ogromnej liczbie urządzeń, a ich proces konfiguracji jest dostępny dla każdego. Po pobraniu aplikacji i utworzeniu konta pozostaje już tylko je aktywować i mniej się martwić, że ktoś włamie się na nasze urządzenie.

Zmiana domyślnej nazwy i hasła routera może również pomóc w zabezpieczeniu sieci. Każdy router jest dostarczany z ogólną nazwą i hasłem, które są potrzebne do skonfigurowania ich po raz pierwszy. Zaraz po tym, dobrą praktyką jest zmiana jego nazwy i hasła na coś unikalnego, pamiętając o wytycznych dotyczących tworzenia silnego hasła. Jest tak, ponieważ nazwy routerów (SSID - service set identifier) najczęściej zawierają w sobie markę i model, co ułatwia hakerom znalezienie routerów, o których wiedzą, że są podatne na naruszenia. Możliwe jest również całkowite ukrycie SSID routera, dzięki czemu szanse na to, że haker dowie się o połączeniu są bliskie zeru.

Źródło: freepik.com

Aktualizuj wszystko. Aktualizacja zwykle wydaje się niepotrzebnym kłopotem, a czasem może nawet pogorszyć funkcjonowanie urządzenia, dodając nowe funkcje,

które nie są potrzebne lub usuwając te, które były przydatne. Ważne jest, aby zwracać uwagę na wszelkie powiadomienia o aktualizacjach, które mogą się pojawić. Każde oprogramowanie nie jest pozbawione wad. Większość z nich zawiera ukryte podatności, z których nawet twórcy nie zdawali sobie sprawy na początku. Po ich znalezieniu mogą one zostać wykorzystane przez hakerów. To jest powód, dla którego każde oprogramowanie potrzebuje nowszych wersji, które mają poprawki w podatnych miejscach. Jest to bardzo ważne z punktu widzenia bezpieczeństwa online, ponieważ utrzymywanie wszystkiego na bieżąco zmniejsza również szanse na udany atak hakerów. Użytkownicy, którzy pilnują regularnego aktualizowania swojego oprogramowania, zmniejszają szanse na cyberatak skierowany na ich urządzenia, ponieważ możliwe jest, że starsze luki, które mogłyby zostać wykorzystane przez hakerów, zostały już naprawione. Istnieje szansa, że aktualizacja może złamać pewne funkcje oprogramowania, a nawet uczynić je bezużytecznym na niektórych urządzeniach, dlatego po aktualizacji dobrze jest sprawdzić, czy aktualizacja niczego nie złamała. Poza tym oprogramowanie, które nie jest aktualizowane, może przegapić nowsze funkcje, które są bardzo wygodne. Z drugiej strony, starsze wersje oprogramowania mogą po prostu przestać działać na nowszych urządzeniach lub tych, które są aktualizowane. Nawet jeśli aktualizowanie rzeczy może wydawać się nieco czasochłonne, jest to bardzo ważne, nie tylko ze względów bezpieczeństwa, ale także ze względu na posiadanie wszystkich najnowszych funkcji danego urządzenia lub oprogramowania. Dobrą praktyką byłoby wykonanie cotygodniowej kontroli używanego oprogramowania pod kątem jego aktualizacji. Jest to naprawdę szybki i prosty sposób na zapewnienie większego bezpieczeństwa danych i zwiększenie wydajności używanego oprogramowania.

Oprogramowanie antywirusowe to konieczność i powinno być zainstalowane na każdym urządzeniu. Nie trudno paść ofiarą ataku phishingowego, a w dzisiejszych czasach, przy rosnącej popularności pracy zdalnej, zainfekowanie komputera wirusem może spowodować przymusową przerwę w pracy na kilka dni, a nawet tygodni. Antywirus to rodzaj oprogramowania, które sprawdza każdy plik lub fragment danych, który jest aktualnie zainstalowany lub jest instalowany na komputerze. Jest on

tworzony w celu określenia, czy któryś z plików znajdujących się na komputerze może być potencjalnym zagrożeniem lub spowodować jakiekolwiek szkody dla użytkowników i ich urządzeń. Antywirus działa na dwa różne sposoby. Jednym z nich jest metoda **oparta na sygnaturach,** która działa jako lista znanych plików zawierających złośliwe oprogramowanie, które są publikowane przez firmy antywirusowe. Po znalezieniu dopasowania między plikiem na liście i na urządzeniu użytkownika, jest on blokowany. Jest to powszechna metoda, która działa dobrze, ponieważ codziennie odkrywane są tysiące złośliwego oprogramowania, więc lista jest naprawdę bogata w dane. Jedynym minusem tej metody jest to, że gdy urządzenie użytkownika zostanie zainfekowane wirusem, którego nie ma na liście, to może nie być przed nim chronione. Innym sposobem, w jaki antywirusy chronią urządzenia, jest metoda **behawioralna**. Jest ona bardziej złożona i nie jest tak powszechnie stosowana jak pozostałe metody, a korzystają z niej tylko najbardziej zaawansowane antywirusy. Jak sama nazwa wskazuje, metoda ta bada zachowanie danego pliku i wydaje osąd czy plik ten może być niebezpieczny dla urządzenia. Sprawdza wszelkie próby modyfikacji lub szyfrowania danych na urządzeniu, a następnie blokuje je, ponieważ flaguje je jako wirusy.

Źródło: freepik.com

Antywirusy chronią użytkowników nie tylko poprzez blokowanie plików, które znajdują się na ich urządzeniach, ale większość z nich blokuje również użytkowników przed wejściem na nieautoryzowane strony, które mogą spowodować ewentualne zagrożenia dla ich urządzeń. Niektóre z tych programów mogą również czyścić tak zwane "pliki śmieci", aby zwolnić trochę miejsca na urządzeniu. Procedura ta może czasami również zwiększyć prędkość przetwarzania danych w komputerze lub smartfonie. Antywirus jest kluczowym elementem każdego urządzenia, które jest podatne na infekcje złośliwymi danymi, i oferuje szeroki wachlarz korzyści, które działają jak zamknięte drzwi, które nie wpuszczają żadnych wirusów do środka i wypuszczają wszystkie istniejące.

Przy zastosowaniu wszystkich tych sugestii niezwykle rzadko zdarza się, że ktoś stanie się ofiarą cyberataku, a nawet jeśli ktoś spróbuje wykraść dane z czyjegoś komputera, jest niezwykle mało prawdopodobne, że mu się to uda.

Rozdział 4 - GDPR a bezpieczeństwo danych osobowych

Ogólne rozporządzenie o ochronie danych (GDPR), które weszło w życie 25 maja 2018 r., miało swoje początki jeszcze w latach 50. ubiegłego wieku. To właśnie wtedy powstała Konwencja Praw Człowieka, która stworzyła pierwsze fundamenty ochrony danych osobowych. Trzy dekady później, wraz z rozwojem komputerów, powstała Konwencja o ochronie danych osobowych, deklarując, że prywatność jest w istocie prawem człowieka. 24 października 1995 r. powstała dyrektywa o ochronie danych osobowych, która regulowała przepisy dotyczące ochrony danych i przekazywania danych osobowych poza granice Unii. 17 lat później zaproponowano aktualizację tych przepisów i po 4 latach od tej propozycji, Ogólne Rozporządzenie o Ochronie Danych zostało przyjęte przez Parlament Europejski, by zaledwie dwa lata później, w maju 2018 roku, stać się w pełni wykonalnym w całej Unii Europejskiej.

Źródło: freepik.com

Istotą GDPR jest zapewnienie obywatelom UE większej kontroli nad ich danymi osobowymi. Jest to ogromny zbiór 99 artykułów regulujących zasady ochrony danych oraz sposób dostępu do danych. Zastąpiła ona poprzednią dyrektywę o ochronie danych z 1995 r. ze względu na fakt, że środowisko technologiczne wyglądało znacznie inaczej niż obecnie. Obecnie prawie każdy Europejczyk posiada przynajmniej jeden smartfon, a firmy oferujące towary lub usługi online stały się równie popularne jak ich tradycyjne odpowiedniki. Dzięki GDPR łatwiej jest kontrolować, jakie dane osobowe mogą być przechowywane, udostępniane lub gromadzone przez różne podmioty.

Informacje te mogą być różne - od adresów IP, przez informacje o miesięcznych dochodach, po nawyki żywieniowe danej osoby.

W ramach GDPR istnieje 7 podstawowych zasad, które powinny być wykorzystywane jako przewodnik po tym, jak należy zarządzać danymi użytkownika. Zasady te mogą być postrzegane jako ramy zaprojektowane w celu pokazania głównego celu regulacji. Wśród tych 7 zasad są:

- Praworządność, uczciwość i przejrzystość.

Oznacza to, że dane muszą być przechowywane i przetwarzane w sposób zgodny z prawem. Nie powinny one wprowadzać w błąd innych użytkowników co do sposobu ich przechowywania i wykorzystania.

- Ograniczenie celu.

Proponuje, aby dane osobowe były zbierane i przechowywane w jasnych, jednoznacznych i zgodnych z prawem celach i nie były dalej przetwarzane w sposób sprzeczny z tymi celami.

- Dokładność.

Oznacza to, że należy podjąć wszelkie uzasadnione środki w celu zapewnienia, że wszelkie dane osobowe, które są niedokładne, zostaną niezwłocznie usunięte lub poprawione. Dane osobowe powinny być dokładne i w razie potrzeby aktualizowane.

- Minimalizacja danych.

Organizacje nie powinny zbierać od swoich użytkowników więcej danych niż potrzebują. Powinny one być adekwatne i ograniczone do tego, co jest niezbędne w odniesieniu do celów, dla których są przetwarzane.

- Ograniczenie przechowywania.

Oznacza, że dane nie powinny być przechowywane dłużej niż jest to konieczne.

- Integralność i poufność.

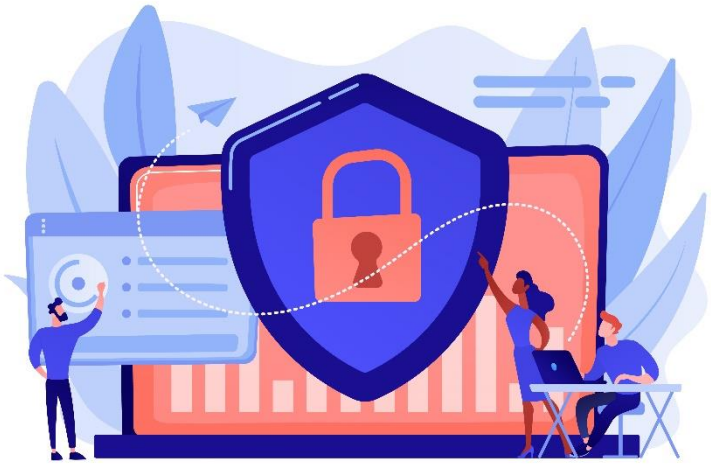
Innymi słowy jest to bezpieczeństwo przechowywanych danych. Powinno być ono przetwarzane z zastosowaniem odpowiednich środków technicznych lub organizacyjnych zapewniających najlepsze bezpieczeństwo danych osobowych, w tym ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przed niezamierzoną utratą, zniszczeniem lub uszkodzeniem.

- Odpowiedzialność.

Oznacza to, że firmy powinny przedstawić dowody na to, że przestrzegają zasad wymienionych powyżej oraz zapewnić, że podejmują środki w celu etycznego postępowania z danymi osobowymi.

GDPR zostało opracowane w celu ochrony użytkowników i ich danych. Pamiętając o tym, zapewnili **osiem praw** dla osób fizycznych. Najistotniejsze z nich to:

- Prawo do informacji na temat gromadzenia i wykorzystywania ich danych osobowych.
- Prawo do dostępu, wglądu i otrzymania kopii swoich danych osobowych, które są gromadzone i przetwarzane przez określone podmioty. Prawo do usunięcia swoich danych osobowych.
- Pozostałe pięć praw osób fizycznych to: prawo do sprostowania, prawo do ograniczenia przetwarzania, prawo do przenoszenia danych, prawo do sprzeciwu oraz prawo do niepodlegania zautomatyzowanemu podejmowaniu decyzji.



Źródło: freepik.com

Ze względu na rosnącą świadomość wartości danych osobowych, ludzie zaczęli zwracać większą uwagę na to, ile danych przekazują firmom i wolą wybierać te strony, które są transparentne w kwestii zbierania danych. Ze względu na GDPR, firmy muszą być bardziej świadome tego, jakie dane gromadzą i jak je zabezpieczają ze względu na wysokie kary związane z nieprzestrzeganiem przepisów GDPR.

Wiedza na temat GDPR wraz z innymi praktykami wymienionymi w tym przewodniku może nie tylko zapewnić wysoki poziom bezpieczeństwa danych osobowych użytkowników, ale także utrudnić cyberprzestępcom włamanie się do baz danych firm. Silne hasła i wiedza na temat różnych złośliwych praktyk, takich jak phishing i wirusy, jeśli zostaną prawidłowo zastosowane i zrozumiane, mogą sprawić, że osoby pracujące zdalnie poczują się znacznie bezpieczniej w czasach, w których telepraca stała się powszechną praktyką na całym świecie.

Rozdział 5 - Działalność praktyczna

Praktyka 1. Tworzenie hasła, które jest silne i łatwe do zapamiętania.

Silne hasło jest długie, skomplikowane i zawiera wiele symboli, ale jest też łatwe do zapamiętania. Mając to na uwadze, stwórzmy je za pomocą tych kilku prostych kroków:

1. Pomyśl o zdaniu lub cytacie, o którym często myślisz. Na przykład słynny cytat Wayne'a Gretzky'ego:
   Pudłujesz 100 procent strzałów, których nie oddajesz.
2. Teraz z tego cytatu utwórz akronim:
   Y(ou) **m**(iss) **100 p**(ercent) **o(**f) **t(**he) **s**(hots) **y**(ou) **d**('ont) **t**(ake) = Ym100potsynt
3. Teraz dodaj do niego znaki specjalne. Na przykład zamieńmy "1" z "!", "p" z "%", dodajmy podkreślenie i zmieńmy wielkość liter, dzięki czemu efekt końcowy będzie wyglądał tak:
   Ym!00%ots_Ydt

Hasło wygląda na skomplikowane, ale jeśli je przeanalizujemy, to zobaczymy, że jest dość proste i łatwe do zapamiętania. Dobrą praktyką jest trenowanie pisania go przez jakiś czas, dzięki czemu nasza pamięć mięśniowa zapamięta kolejność wciskanych przycisków.

Źródło: freepik.com

Praktyka 2. Sprawdzaj swoją skrzynkę pocztową pod kątem SPAMu i ewentualnych prób phishingu.

Poznaliśmy różne złośliwe e-maile, które mogą być do nas wysłane i jak je rozpoznać.

Otwórz swoją skrzynkę pocztową i sprawdź, czy nie ma w niej reklam produktów, o których nigdy nie słyszałeś lub powiadomień o wygraniu jakiejś nagrody. Sprawdź też, czy nie ma podejrzanych e-maili o niezapłaconych fakturach lub zawieszeniu konta. Przeanalizuj je, ale pod żadnym pozorem **NIE** otwieraj żadnych linków ani załączników podanych w wiadomościach. Następnie skasuj te wiadomości i zastanów się, ile było tych podejrzanych maili.

Przydatne linki:

Jak bezpieczne jest twoje hasło:
https://www.security.org/how-secure-is-my-password/

Jak zainstalować połączenie VPN:
https://www.businessnewsdaily.com/15710-how-to-install-a-vpn-connection.html

4. Referencje

Anderson, S. (2022). *What Is Phishing? Przewodnik z przykładami na rok 2022*. SafetyDetectives. Retrieved May 10, 2022, from https://www.safetydetectives.com/blog/what-is-phishing-and-how-to-protect-against-...

Awati, R., & Teravainen, T. (2021). *Czym jest spam mailowy i jak z nim walczyć?* SearchSecurity. Retrieved May 9, 2022, from https://www.techtarget.com/searchsecurity/definition/spam?msclkid=9aeb4557cf8211ec82e6cfc07708ec54.

Barracuda. (2020). *Spear Phishing: Top Threats and Trends* (Vol. 5). Barracuda. Retrieved May 10, 2022, from https://lp.barracuda.com/rs/326-BKC-432/images/BEU-AMER-Spear-Phishing-Vol5...

Castagna, R., & Lavery, T. (2021). *Ogólne rozporządzenie o ochronie danych osobowych (GDPR)*. WhatIs.Com. Retrieved June 24, 2022, from https://www.techtarget.com/whatis/definition/General-Data-Protection-Regulation-GDPR.

Cheema, A. N., & Aamir, R. (2021). Trendy w zakresie cyberprzestępczości. *Proc. 18th International Conference on Statistical Sciences*, *35*, 261-269. https://www.researchgate.net/profile/Muhammad-Suhail-6/publication/353070981_Comparison_of_Ridge...

Chng, S., Han Yu, L., Kumar, A., & Yau, D. (2022). Typy hakerów, motywacje i strategie: A comprehensive framework. *Computers in Human Behavior Reports*, *5.* https://doi.org/10.1016/s2451-9588(22)00018-5

Digital Marketing Experts - Editorial Review Board. (2021). *The Importance of Updating*. TAK!!! Company. Retrieved June 24, 2022, from https://www.thatcompany.com/the-importance-of-updating...

D'Mello, Y. (2018). *Jak się tu znaleźliśmy? Krótka historia GDPR*. AiThority. Retrieved June 24, 2022, from https://aithority.com/technology/analytics/how-did-we-get-here-a-brief-history-of-the-gdpr/.

Edwards, R. (2022). *Jak mogę zabezpieczyć swoje połączenie internetowe?* SafeWise. Retrieved June 24, 2022, from https://www.safewise.com/online-security-faq/secure-internet-connection/.

Elvin, A. E., Sundström, F., & von Heland, W. (2021). *Understanding the Effects of Cyber Security Risks and Threats on Forced Teleworking Organizations* (Master's dissertation). Wydział Informatyki, Lund School of Economics and Management, Lund University. Retrieved June 24, 2022, from https://lup.lub.lu.se/student-papers/search/publication/9052971.

Technologia informacyjna FIT. (2022). *Co to jest antywirus i dlaczego jest ważny?* Retrieved June 24, 2022, from https://it.fitnyc.edu/what-is-antivirus-and-why-is-it-important/.

Fogg, S. (2022). *Co to jest GDPR? Podstawy unijnego ogólnego rozporządzenia o ochronie danych osobowych*. Termly. Retrieved June 24, 2022, from https://termly.io/resources/articles/what-is-gdpr/.

Fruhlinger, J. (2020). *Ransomware wyjaśnione: Jak działa i jak je usunąć*. CSO Online. Retrieved May 11, 2022, from https://www.csoonline.com/article/3236183/what-is-ransomware-how-it-works-and-how-to-remove-it...

Gajić, A. (2022). *Statystyki spamu*. 99firms. Retrieved May 9, 2022, from https://99firms.com/blog/spam-statistics/?msclkid=18264839cf8b11ec8144c5ced7add618.

Ogólne rozporządzenie o ochronie danych (GDPR) - oficjalny tekst prawny. (2019). Ogólne rozporządzenie o ochronie danych (GDPR). Retrieved June 24, 2022, from https://gdpr-info.eu/.

Gibson, K. (2022). *6 słynnych przypadków kradzieży tożsamości w ostatnich latach*. Home Security Heroes. Retrieved May 12, 2022, from https://www.homesecurityheroes.com/famous-identity-theft-cases/

Gupta, M. (2021). Kradzież tożsamości w cyberprzestrzeni w Indiach. *International Journal of Research Publication and Reviews*, *2*(7), 1700-1701. https://www.ijrpr.com/uploads/V2ISSUE7/IJRPR791.pdf

Hiley, C. (2021). *Krótka historia cyberbezpieczeństwa i hakingu*. CyberNews. Retrieved May 11, 2022, from https://cybernews.com/security/brief-history-of-cybersecurity-and-hacking/?msclkid=ebaaa52cd10911ecbb48b6bc018d0384.

Jančis, M. (2022). *Jak stworzyć dobre i silne hasło*. CyberNews. Retrieved June 16, 2022, from https://cybernews.com/best-password-managers/how-to-create-a-strong-password/.

Janssen, D. (2022). *VPN Explained: How Does It Work? Why Would You Use It?* VPNoverview.Com. Retrieved June 1, 2022, from https://vpnoverview.com/vpn-information/what-is-a-vpn/

Johansen, A. G. (2018). *What to Do If Your Identity Is Stolen: 14 Steps*. LifeLock. Retrieved May 12, 2022, from https://www.lifelock.com/learn/identity-theft-resources/do-these-things-immediately-if-your-identity-has-been-stolen.

Lopez, A. (2021). *Top 10 Reasons Why an Antivirus Is Important*. Business 2 Community. Retrieved June 24, 2022, from https://www.business2community.com/cybersecurity/top-10-reasons-why-an-antivirus-is-important...

Malwarebytes. (n.d.). *Czym jest spam?* Retrieved May 11, 2022, from https://www.malwarebytes.com/spam...

Martens, B. (2021). *The Ultimate Internet Safety Guide for Seniors (2022)*. SafetyDetectives. Retrieved June 24, 2022, from https://www.safetydetectives.com/blog/the-ultimate-internet-safety-guide-for-seniors/?msclkid=9e7ed272cf5f11ecbe3d195abee11879.

Milasi, S., González-Vázquez, I., & Fernández-Macías, E. (2020). *Telepraca w UE przed i po konferencji COVID-19: Gdzie byliśmy, dokąd zmierzamy*. Wspólne Centrum Badawcze. Retrieved June 24, 2022, from https://joint-research-centre.ec.europa.eu/system/files/2021-06/...

Minahan, B. (2020). *How to Create* a *Strong Password in 6 Easy Steps*. aNetworks. Retrieved June 1, 2022, from https://www.anetworks.com/how-to-create-a-strong-password-2021/.

Mitra, A. (2017). *Czym jest spambot i jak powstrzymać spamboty?* TheSecurityBuddy. Retrieved May 11, 2022, from https://www.thesecuritybuddy.com/anti-spam/what-is-spambot-and-how-to-stop-spambots...

Molinaro, D. (2022). *Jak działa uwierzytelnianie dwuskładnikowe (2FA)?* Avast. Retrieved June 1, 2022, from https://www.avast.com/c-how-does-two-factor-authentication-work...

Movassagh, N. (2021). *Świadomość i postrzeganie wariantów phishingu przez studentów Policing, Computing i Criminology w Canterbury Christ Church University.* (Master's dissertation). Canterbury Christ Church University School of Law. https://repository.canterbury.ac.uk/item/8yq89/awareness-and-perception-of-phishing-variants-from-policing-computing-and-criminology-students...

Peterson, S. (2019). *The Ultimate Guide for Online Security and Privacy in 2020*. The Hack Post. Retrieved June 1, 2022, from https://thehackpost.com/the-ultimate-guide-for-online-security-and-privacy-in-2020.html.

Proofpoint. (n.d.). *Co to jest Email Spoofing? Definition & Examples*. Retrieved June 24, 2022, from https://www.proofpoint.com/us/threat-reference/email-spoofing?msclkid=df4910a2d03511ecb958bcffa531b6ab

Spoofing i Phishing. (2022). Federal Bureau of Investigation. Retrieved May 10, 2022, from https://www.fbi.gov/scams-and-safety/common-scams-and-crimes/spoofing-and-phishing?msclkid=8cb3cf19d04d11ecb7c47a9f8893c5e8.

Tanwar, R., Choudhury, T., Zamani, M., Gupta, S., & Tajpour, A. (2021). Bezpieczeństwo informacji a optymalizacja. In *Bezpieczeństwo informacji i optymalizacja* (pp. 25-26). CRC Press. Retrieved May 10, 2022, from https://books.google.nl/books?id=...

TechFunnel Contributors. (2020). *Najczęstsze techniki hakerskie dla początkujących*. Techfunnel. Retrieved May 11, 2022, from https://www.techfunnel.com/information-technology/hacking-techniques/?msclkid=94348692d12111eca373f0ead6ff7fe9.

Tschabitscher, H. (2021). *What Is an Example of Spam Email?* Lifewire. Retrieved May 9, 2022, from https://www.lifewire.com/what-and-why-spam-email-1173993#toc-what-are-some-examples-of-spam.

Tsonchev, A. (2020). *Sześć największych zagrożeń bezpieczeństwa, przed którymi stoją pracownicy zdalni*. TechRadar. Retrieved June 24, 2022, from https://www.techradar.com/news/six-of-the-biggest-security-threats-facing-the-remote-workforce?msclkid=9e80a80ccf5f11ec92c0ce7275373494.

Williams, L. (2022). *Co to jest Hacking? Rodzaje hakerów | Wprowadzenie do cyberprzestępczości*. Guru99. Retrieved June 24, 2022, from https://www.guru99.com/what-is-hacking-an-introduction...

Zdjęcie strony tytułowej źródło: freepik.com