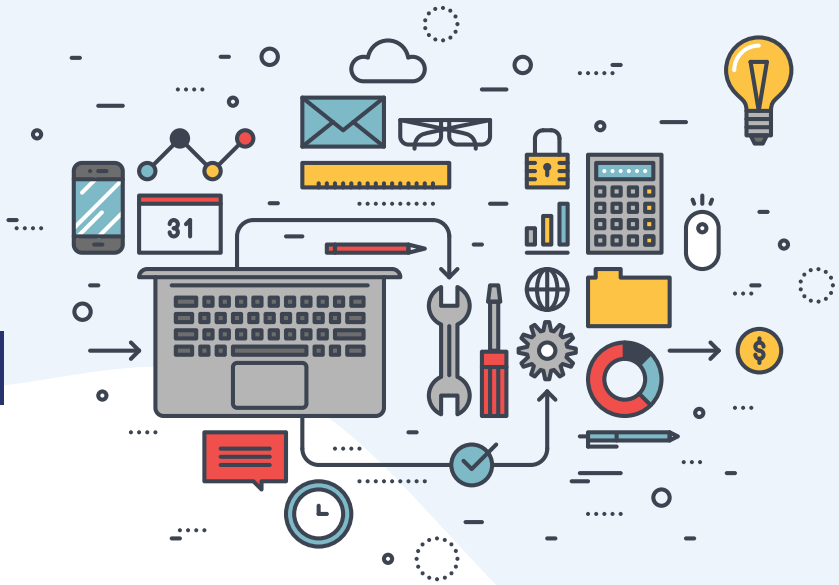
Bezpieczna praca zdalna

WSKAZÓWKI I PORADY DLA PRACODAWCÓW



Ustal zasady i procedury w firmie (przetestuj je wcześniej, jeśli to możliwe)

Zapewnij jasne zasady dotyczące pracy zdalnej, w tym dostęp do zasobów firmy i osób kontaktowych w przypadku problemów. Ustal przejrzystą procedurę w przypadku wystąpienia incydentu bezpieczeństwa.

Zastosuj dodatkowe środki bezpieczeństwa dla pracowników szczebla kierowniczego związane z obiegiem dokumentacji, zatwierdzaniem/informacją zwrotną czy przekazywaniem informacji.

Zabezpiecz sprzęt firmowy

Zastosuj środki bezpieczeństwa, takie jak szyfrowanie dysku twardego, wylogowanie automatyczne po okresie bezczynności, filtry prywatyzujące, silne uwierzytelnianie i kontrolę oraz szyfrowanie wymiennych nośników danych (np. dyski USB).

Wyposaż sprzęt w opcję zdalnego dezaktywowania na wypadek zagubienia lub kradzieży.

Bezpieczny dostęp zdalny

Zezwalaj swoim pracownikom na łączenie się z siecią firmową wyłącznie za pośrednictwem służbowego VPN z uwierzytelnianiem wieloetapowym.

Wprowadź wymóg ponownego logowania do zdalnej sesji, aktywowany automatycznie po określonym okresie bezczynności.

Aktualizuj systemy operacyjne i aplikacje

Pomoże to zmniejszyć ryzyko ataku cyberprzestępców wykorzystujących luki w zabezpieczeniach.

Zabezpiecz komunikację w swojej firmie

Zastosuj uwierzytelnianie wieloetapowe w celu uzyskania dostępu do służbowych kont e-mail. Zapewnij dostęp do bezpiecznych kanałów komunikacji dla pracowników, aby łatwo mogli się komunikować między sobą, a także z klientami zewnętrznymi.

Monitoruj stan bezpieczeństwa firmy

Sprawdzaj nietypowe działania pracowników pracujących zdalnie i zwiększaj poziom zabezpieczenia w przypadku ataków związanych z VPN.

Uświadamiaj pracownikom zagrożenia związane z pracą zdalną

Edukuj pracowników na temat polityki firmy dotyczącej pracy zdalnej. Poświęć czas na podniesienie poziomu świadomości na temat cyberzagrożeń, zwłaszcza takich jak phishing i socjotechnika.

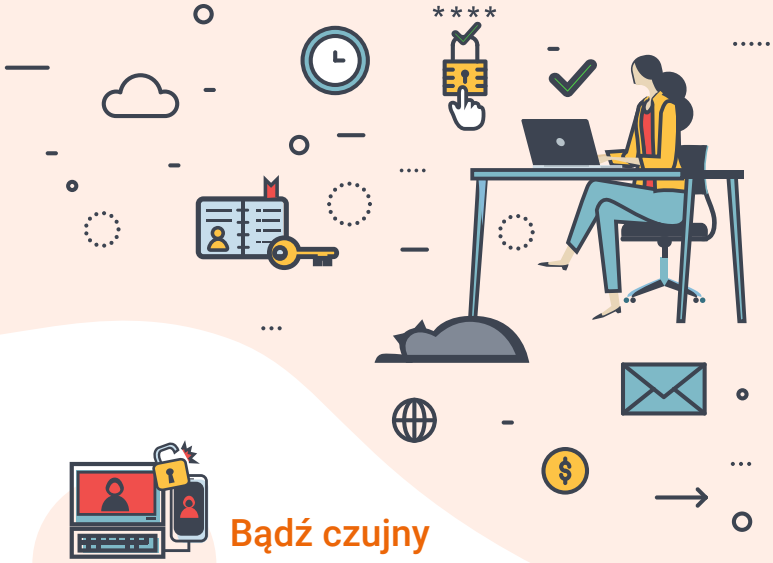
Regularnie kontaktuj się z pracownikami

Wyznacz konkretne cele, harmonogram pracy i mechanizmy monitorowania, w miarę możliwości elastycznie, biorąc pod uwagę okoliczności.

NASK POLICJA EUROPOL EC3 European Cybercrime Centre

Bezpieczna praca zdalna

WSKAZÓWKI I PORADY DLA PRACOWNIKÓW



Używaj wyłącznie sprzętu pracodawcy w celu dostępu do firmowych danych

Używaj wyłącznie urządzeń i oprogramowania dostarczonych przez pracodawcę.

Utwórz silne hasła (użyj zaufanego / uznanego menedżera haseł, jeśli to możliwe), nie zapisuj haseł na karteczkach i pilnuj aby nikt nie widział kiedy wprowadzasz je do sytemu. Nie korzystaj z obejść systemu, nawet jeżeli ułatwiają Ci pracę.

Stój. Pomyśl. Połącz

Przed rozpoczęciem pracy zdalnej zapoznaj się ze sprzętem firmowym, poznaj zasady i procedury bezpieczeństwa. Upewnij się, że dobrze znasz sprzęt, rozumiesz zalecenia i zakazy związane z jego użyciem i wiesz gdzie szukać pomocy w razie problemów.

Bezpieczny dostęp zdalny

Łącz się z siecią firmową tylko przez firmowy VPN i chroń urządzenia niezbędne do nawiązania bezpiecznego połączenia np. tokeny czy karty.

Chroń sprzęt i środowisko pracy

Nie pozwalaj członkom rodziny na dostęp do sprzętu firmowego. Zablokuj lub wyłącz sprzęt, gdy pozostawiasz go bez nadzoru i zawsze przechowuj w bezpiecznym miejscu, aby zapobiec utracie, uszkodzeniu lub kradzieży. Używaj filtrów prywatyzujących i unikaj ustawiania ekranów w kierunku okien lub kamer.

Zgłaszaj/ Informuj

Jeśli zauważysz jakieś nietypowe lub podejrzane działania na dowolnym urządzeniu, którego używasz do pracy zdalnej, natychmiast skontaktuj się ze swoim pracodawcą za pośrednictwem odpowiednich kanałów komunikacji.

Bądź czujny

Uważaj na wszelkie podejrzane działania i polecenia, zwłaszcza te związane z realizacją czynności finansowych w Internecie. Ktoś może podszywać się pod współpracownika lub przełożonego! W razie wątpliwości osobiście zadzwoń do osoby wysyłającej prośbę, aby dokładnie wszystko sprawdzić.

Jeśli nie wiesz dlaczego dany e-mail lub sms trafił do ciebie, nie klikaj linków ani załączników, które w nim są.

Unikaj udostępniania danych osobowych

Nigdy nie podawaj żadnych danych osobowych w korespondencji, nawet jeśli prośba pochodzi z wiarygodnego źródła. Zamiast tego skontaktuj się bezpośrednio z osobą kierującą do Ciebie korespondencję, w celu potwierdzenia zapytania.

Opracuj nowe zasady/procedury

W okresie pracy zdalnej, omów plan prac ze swoim bezpośrednim przełożonym i członkami zespołu, w tym podział zadań, terminy i kanały komunikacji.

Używanie własnego sprzętu

Jeśli korzystanie z prywatnego urządzenia jest jedyną opcją, a pracodawca na to zezwala, upewnij się, że system operacyjny i oprogramowanie urządzenia są aktualne, zawierają program antywirusowy oraz chroniący przed malware, a połączenie jest zabezpieczone przez VPN zatwierdzony przez Twoją firmę.

Oddzielaj pracę od czasu wolnego

Unikaj używania sprzętu firmowego do celów prywatnych.

NASK POLICJA EUROPOL EC3 European Cybercrime Centre