CYBERSECURITY AWARENESS MONTH

CYBERBEZPIECZEŃSTWIO NA CO DZIEŃ (SEE YOURSELF IN CYBER)

Wszyscy mamy wpływ na cyberbezpieczeństwo... niezależnie od pełnionej funkcji.

Wnieś wkład w cyberbezpieczeństwo własne i swojej firmy, stosując się do czterech podstawowych zasad.

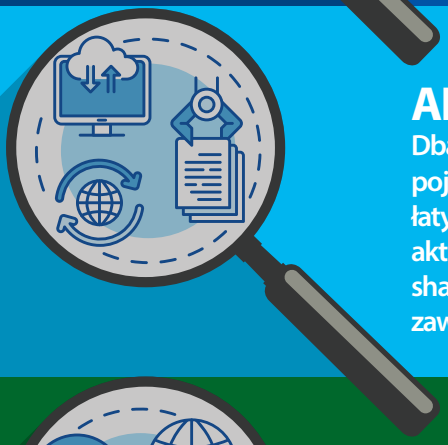
STOSUJ UWIERZYTELNIANIE WIELOCZYNNIKOWE

Uwierzytelnianie wieloczynnikowe, znane również pod nazwą uwierzytelniania dwuskładnikowego lub weryfikacji dwuetapowej, jest środkiem bezpieczeństwa, polegającym na wymaganiu od osób logujących się na konto przejścia dwuetapowej procedury potwierdzania tożsamości. Sprawia to, że przestępca ma dwa razy trudniejszy dostęp do konta. Przez dodanie jednego prostego etapu logowania się na konto, uwierzytelnianie wieloskładnikowe znacznie zwiększa bezpieczeństwo.

UŻYWAJ SILNYCH HASEŁ

Jeśli dane mają być bezpieczne, ważne jest stosowanie odpowiednich haseł. Oto kilka prostych sposobów zabezpieczenia konta przez stosowanie lepszych haseł. Niezależnie od rodzaju konta, hasła należy tworzyć, pamiętając o tych trzech słowach.

- Długie – co najmniej 12 znaków
- Niepowtarzalne – do każdego konta należy używać innego hasła
- Złożone - w haśle używaj i dużych, i małych liter, cyfr oraz znaków specjalnych. Na niektórych stronach internetowych w hasłach można nawet używać spacji.



AKTUALIZUJ OPROGRAMOWANIE

Dbaj, aby twoje oprogramowanie było zawsze aktualne, instaluj aktualizacje, gdy tylko się pojawiają, nie zwlekaj. Aktualizacje eliminują ogólne problemy z programem i zawierają nowe łaty bezpieczeństwa w miejscach, przez które mogliby włamywać się przestępcy. Pobieraj aktualizację wyłącznie od firm, które tworzyły dane oprogramowanie. Nigdy nie korzystaj ze shakowanych, pirackich lub nielicencjonowanych wersji oprogramowania, ponieważ często zawierają one złośliwe programy i raczej powodują problemy, niż je rozwiązują.

ZWRACAJ UWAGĘ NA OSZUSTWA TYPU PHISHING I ZGŁASZAJ JE

Oznaki tego mogą być mało widoczne, ale gdy rozpoznasz próbę phishingu, możesz uniknąć nabrania się na takie oszustwo. Oto kilka prostych wskazówek, jak rozpoznać fałszywy e-mail, będący próbą phishingu: Zawiera ofertę, która jest zbyt korzystna, aby być prawdziwą; sformułowania, które są ponaglające lub alarmujące, albo zawierają groźbę; tekst jest napisany niepoprawnie, zawiera błędy ortograficzne i gramatyczne; powitania są niejednoznaczne lub bardzo ogólne; w wiadomości jest prośba o wysłanie danych osobowych; ponaglenie do kliknięcia nieznanego hiperłącza lub otwarcia załącznika; widoczne są dziwne lub niespodziewane prośby biznesowe; adres nadawcy jest niezgodny z nazwą firmy rzekomo wysyłającej e-mail.

MAUSER
Packaging Solutions