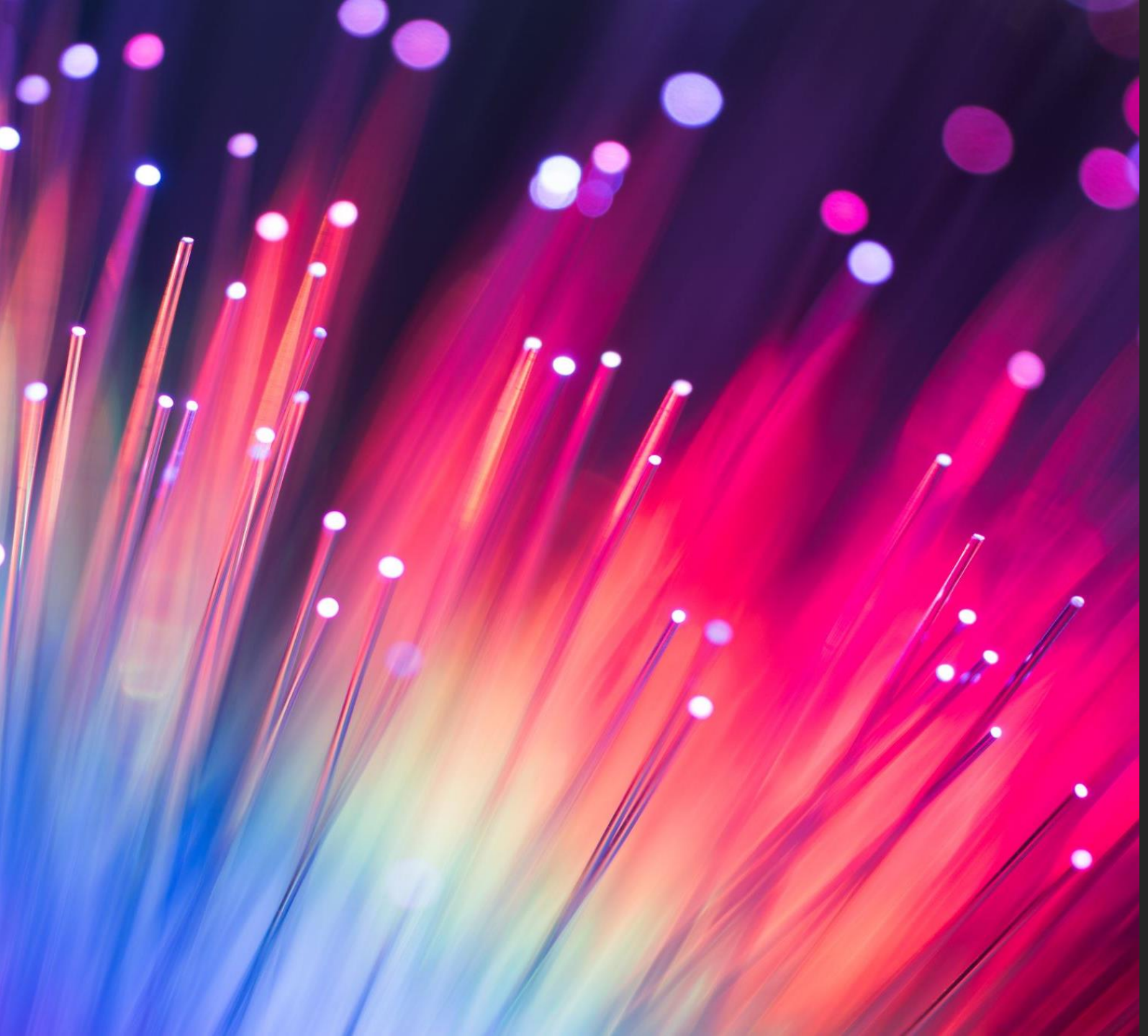

BEZPIECZNY INTERNET

NAJWAŻNIEJSZE ZASADY BEZPIECZEŃSTWA W SIECI

JAN MOZIŃSKI KLASA 6B

(ANTY)WIRUSY

Podstawą bezpiecznego korzystania z Internetu jest zainstalowanie w porządnego oprogramowania antywirusowego. Ustrzeże nas ono przed dużą ilością przykrych konsekwencji, które niesie za sobą ludzka złośliwość; Pomoże uchronić nasz komputer. Program antywirusowy zawczasu wykryje złośliwe oprogramowanie czy obecność wirusa i nie pozwoli im zagościć w naszym komputerze, Niemniej jednak nawet posiadając program do ochrony przed wirusami, warto z rozwagą pobierać pliki z sieci oraz nie otwierać nieznanych załączników w mailach, które budzą nasze zaniepokojenie. Niestosowanie Anty-Wirusa może spowodować, że przez wirusa stracimy ważne dane, zdjęcia i inne informacje osobowe, często dla nas bardzo ważne.

DANE OSOBOWE

Nieuważne zgody na przetwarzanie danych osobowych lub na otrzymywanie informacji marketingowych mogą w konsekwencji prowadzić do tragicznych w skutkach wydarzeń: kradzieży tożsamości lub próby wyłudzenia kredytu. Najczęściej takie dane jak imię, nazwisko i adres podajemy podczas zakupów w sieci. Nasz niepokój powinna wzbudzić zbyt duża ilość wymaganych danych (np. PESEL, adres zameldowania itp.). Zaznaczenie zgody na przetwarzanie danych osobowych powoduje przede wszystkim utratę kontroli nad tym co stanie się z nimi w przyszłości. Dane gromadzone przez firmy są często odsprzedawane innym podmiotom gospodarczym, które nękają później ich właścicieli wielością ofert lub ankiet.

INTERNETOWI PRZYJACIELE

Coraz częściej poznajemy ludzi przez Internet. W wirtualnej rzeczywistości można zawrzeć wartościowe i ciekawe znajomości; Pamiętajmy jednak, że nigdy nie wiadomo kto siedzi po drugiej stronie; Dlatego nie należy przesadzać z nadmierną wylewnością w takich relacjach. Anonimowość, którą daje wirtualna rzeczywistość staje się niekiedy płaszczem dla przestępców, złodziei oraz innych ludzi o nieczystych intencjach. Warto o tym pamiętać. Do wszelkich znajomości zawieranych w Internecie należy podchodzić w ostrożnością.

HASŁA DOSTĘPU I LOGOWANIE. CERTYFIKAT SSL

Nikomu pod żadnym pozorem nie należy podawać swoich haseł. Powinny być one trudne do odszyfrowania i składać się ze skomplikowanej kombinacji dużych i małych liter, cyfr oraz znaków specjalnych. Niezwykłą wagę należy przykładać przede wszystkim do ochrony kont bankowych, skrzynki mailowej, kont w serwisach społecznościowych; Czyli wszędzie tam, gdzie można odnaleźć swobodny dostęp do naszych danych wrażliwych, bazy zdjęć i innych informacji, które ktoś mógłby wykorzystać przeciwko nam. Jeśli na jakiejkolwiek stronie wyświetla nam się jej regulamin – warto go przeczytać. Warto zawsze sprawdzić wiarygodność strony, z której korzystamy; Tutaj z pomocą przychodzi tak zwany certyfikat SSL - jest to protokół sieciowy używany do nawiązywania bezpiecznych połączeń internetowych. Oznacza to, że za pomocą SSL mogą być szyfrowane połączenia do poczty, strony WWW itp.