Najczęściej spotykane rodzaje cyberataków, o których należy wiedzieć:

- Phishing

Phishing jest to oszustwo stosowane przez cyberprzestępców w celu uzyskania cennych informacji, takich jak: loginy i hasła, numery kart kredytowych, czy numer PESEL. W tego rodzaju przestępstwa wykorzystuje się najczęściej fałszywe e-maile i SMS-y. Coraz częściej oszuści działają także za pośrednictwem komunikatorów i portali społeczności. Aby wzbudzić zaufanie potencjalnej ofiary, phisherzy podszywają się pod powszechnie rozpoznawalne firmy i instytucje, tj.: banki, urzędy, portale aukcyjne, firmy kurierskie czy telekomunikacyjne. Za pomocą spreparowanych wiadomości próbują nakłonić ofiarę do kliknięcia w umieszczony w wiadomości link, który z reguły prowadzi do strony internetowej stworzonej przez cyberprzestępców. Strona www jest łudząco podobna do autentycznej witryny firmy czy instytucji, od której rzekomo pochodzi wiadomość , jednak stanowi pułapkę zastawioną na nieostrożnych internautów.

Jak się chronić? Przede wszystkim należy stosować zasadę ograniczonego zaufania. Odruchowe klikanie w linki i pobieranie plików z nieznanych źródeł jest bardzo ryzykownym zachowaniem – przed otworzeniem wiadomości zastanówmy się czy np. oczekujemy na przesyłkę. Pod żadnym pozorem nie udostępniajmy innym osobom loginów i haseł. Fałszywe wiadomość bardzo często zawierają błędy ortograficzne, gramatyczne i interpunkcyjne. Adresy mailowe, którymi posługują się oszuści, mogą się różnić od tych autentycznych łatwymi do przeoczenia szczegółami, np. literówką w nazwie domeny.

- Złośliwe oprogramowanie

Złośliwe oprogramowanie często przedostaje się do komputerów, podszywając się pod zupełnie niewinne załączniki wiadomości e-mail lub fałszywe przyciski na stronach internetowych. Umożliwia mu to obejście zabezpieczeń sieci. Tego typu oprogramowanie, znane jako oprogramowanie szpiegujące, może również przesyłać dane osobowe, instalować kolejne złośliwe programy lub całkowicie wyłączać komputer.

Jak się chronić? By zapewnić bezpieczeństwo komputera, powinno się pobierać wyłącznie te pliki, co do których mamy pewność.

- Ransomware

Ransomware to rodzaj złośliwego oprogramowania szyfrującego wszystkie pliki. Trudno jest rozpoznać, że akurat pobiera się ransomware. Często wyląduje ono w skrzynce odbiorczej pod niewinną nazwą pliku od niewinnie brzmiącego nadawcy. Po jego otwarciu dostęp do plików stanie się niemożliwy, a by go odzyskać, trzeba będzie zapłacić okup.

Jak się chronić? Oprogramowanie antywirusowe powinno być zaktualizowane i aktywne przez cały czas. Bardzo przydatne jest regularne tworzenie backupów ważnych plików i trzymanie ich na urządzeniach, które nie są permanentnie podłączone do komputera. Jeśli padniemy ofiarą ransomware, możemy odzyskać pliki z backupu, zamiast płacić za klucz do deszyfrowania swoich plików.

- Atak Man-in-the-Middle

Atak MITM – (ang. Man in the Middle) to nic innego, jak prosty atak sieciowy, którego zamysłem jest podsłuchiwanie wymiany danych pomiędzy stronami komunikacji lub ewentualnej jej modyfikacji. Wyróżnia go brak świadomości użytkownika o podsłuchu oraz to, że informacje, które otrzymuje lub, które wysyła mogą być zmodyfikowane przez cyberprzestępcę.

Jak się chronić? Starajmy się unikać publicznych sieci Wi-Fi. Zaopatrzmy nasz sprzęt w oprogramowanie antywirusowe, skutecznie radzą sobie z atakami Man in the middle. Aktualizujmy swoją przeglądarkę – coraz więcej przeglądarek ma wbudowane mechanizmy obronne.

- Ataki DDoS (Denial of Service)

Atak DDoS ma miejsce wtedy, gdy sieć lub serwer są przeciążone i zalane dużą ilością danych internetowych. Przy tak wielkim nagromadzeniu danych wykorzystujących przepustowość sieci nie możesz normalnie z niej korzystać. Ten rodzaj ataku jest najczęściej kierowany na strony internetowe firm i organizacji. Celem tych ataków raczej nie są pieniądze, a utrudnienie dostępu klientom i osobom odwiedzającym stronę.

Jak się chronić? Sposobem ochrony są przede wszystkim programy antywirusowe chroniące zarówno samodzielne komputery jak i całe sieci zapewniając wielopłaszczyznowe formatowanie. Równie ważne jest stosowanie regularnej aktualizacji aplikacji internetowych, by w razie ataku niemożliwe było wykorzystanie luk w ich budowie. Zaleca się także ostrożność podczas korzystania z poczty. Zanim otworzy się wiadomość, należy dokładnie sprawdzić nadawcę i szczegóły wiadomości.