Zasady bezpiecznego korzystania z komputera

Z raportu CERT Polska wynika, że poruszanie się w Internecie wymaga coraz więcej ostrożności. W cięgu jednego roku liczba zarejestrowanych incydentów wzrosła aż o 73%. Przestępcy wcięż cenię sobie sprawdzone metody - najchętniej sięgają po phishing.

Niezależnie czy prowadzisz firmę, jesteś pracownikiem, prowadzisz gospodarstwo rolne czy po prostu przechowujesz rodzinne zdjęcia to stosowanie tych rad pozwoli uniknąć Ci kłopotów związanych z działalnością komputerowych przestępców.
Jak być bezpiecznym:
1. Chroń swoje dane osobowe. Pamiętaj, że istnieją metody i narzędzie ochrony Twoich danych przesyłanych w komputerowych plikach. Wiele narzędzi jest bezpłatnych. Wystarczy tylko po nie sięgnąć aby uchronić swoje dane przed komputerowymi przestępcami.
2. Korzystaj z oprogramowania antywirusowego a jeżeli to możliwe to również z oprogramowania antyszpiegowskiego, zapory ogniowej i regularnie je aktualizuj.
3. Aktualizuj na bieżąco swój system operacyjny i przeglądarkę internetową.
4. W bezpieczny sposób usuwaj swoje dane z nośników.
5. Stosuj zasadę „czystego ekranu" (nie pozostawiaj otwartych dokumentów zawierających dane, które mogłyby wejść w „niepowołane ręce").
6. Jakiekolwiek hasła, piny staraj się pamiętać – niedozwolone jest trzymanie ich na biurku lub w łatwo dostępnym miejscu – np. pod klawiaturą czy podkładką na biurko. Haseł nie podajemy nikomu!
7. Do przechowywania haseł dostępu stosuj tzw. magazyny haseł (m.in. KeePass) oraz generatory haseł (do ich tworzenia). Najlepiej wykorzystać generatory ze stron producentów oprogramowania antywirusowego lub VPN.
8. Hasła do komputera powinny składać się z min. 11 znaków, duże litery + małe litery + cyfry i znaki specjalne, nie powinny być banalne np. „1234", nazwisko_uzytkownika", itp. Zabronione jest stosowanie haseł zawierających nazwy własne lub jakiekolwiek frazy słownikowe. Nie stosujemy haseł zawierających informacje nt. imion dzieci czy innych wydarzeń z naszego prywatnego życia.

9. Hasła powinny być zmieniane co 30 dni lub w czasie gdy wymusza to kontroler domeny, serwer, aplikacja dziedzinowa. Nie zmieniamy hasła w sposób polegający na zmianie wyłącznie ostatniego znaku (ów). Z badań wynika, że podczas konstrukcji „trudnych" haseł wykorzystujemy dwie pierwsze duże litery. Na końcu hasła za to chętnie wstawiamy wykrzyknik. Jeżeli Twoje hasło zostało wytworzone w ten sposób to zmień je.

10. Nigdy, pod żadnym pozorem nie stosuje jednego hasła do wszystkich serwisów, z których korzystasz. Jeżeli przestępcy zdobędą Twoje dane logowania do np. poczty elektronicznej sprawdzą, czy uda im się z wykorzystaniem tego samego hasła zalogować np. do Twojego konta na Facebooku. Jeżeli tak, ukradną całą Twoją tożsamość. Pomyśl, jakie mogą być skutki takiego działania!

10. Sprawdzaj, czy Twoje konta (pocztowe, do portali społecznościowych) nie zostały skradzione. Wejdź na stronę https://haveibeenpwned.com/ i sprawdź, czy Twój adres e-mail został skradziony a Twoje dane logowania skompromitowane. Jeżeli przestępca nie zdążył jeszcze wykorzystać Twojego konta a Ty nadal masz do niego dostęp NATYCHMIAST ZMIEŃ HASŁO. Zmień hasła również w innych serwisach – jeżeli było takie samo jak do poczty. Pamiętaj o zasadach tworzenia dobrych haseł.

11. Aktualizuj oprogramowanie swoich urządzeń pracujących na styku sieci (routerów). Jeżeli masz bardzo stary router – wymień go. To urządzenie nie jest już bezpieczne!

12. Nie korzystaj z otwartych sieci WIFI aby uniknąć ataku typu man in the middle (człowiek po środku). Jeżeli już musisz skorzystać z otwartej sieci WIFI na dworcu lub lotnisku stosuj rozwiązania typu VPN.

13. Gdy musimy odejść od komputera (chronionego hasłem) a na ekranie znajdują się dane firmowe (klientów, kontrahentów) – blokujemy ekran (wciskamy na klawiaturze jednocześnie klawisze Win oraz L)

14. Używaj wyłącznie licencjonowanego oprogramowania – programy pirackie często zawierają wirusy, poza tym ich wykorzystywanie niezależnie od miejsca wykorzystania (dom, praca, szkoła) to przestępstwo.

15. Nie wchodź na strony zawierające treści niedozwolone (np. z pirackim oprogramowaniem) – istnieje ryzyko złapania wirusa.

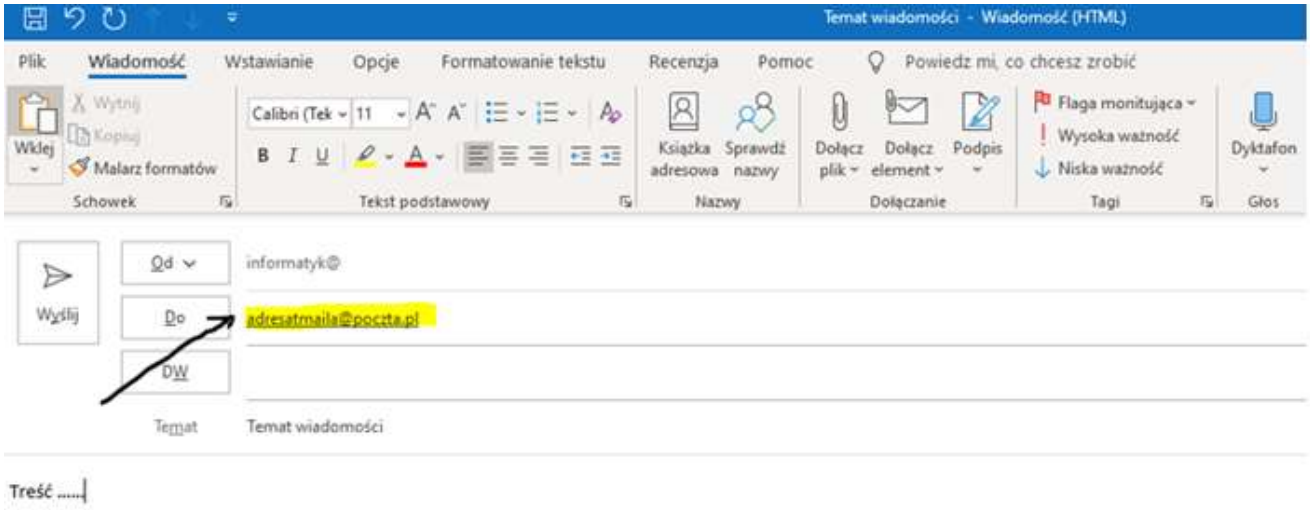
16. Nie należy w opcjach przeglądarki internetowej włączać opcji autouzupełniania formularzy i zapamiętywania haseł. Po zakończonej pracy wylogowujemy się z poszczególnych systemów – dużo osób nie wylosowuje się z poczty.

17. Dokumenty zawierające dane poufne niszczymy w niszczarkach spełniających normę P-3, dawniej DIN 3. Nigdy nie wyrzucamy dokumentów zawierających dane poufne lub osobowe bezpośrednio do kosza na śmieci.

18. Na bieżąco twórz kopie bezpieczeństwa danych w sposób uniemożliwiający ingerencję w dane złośliwego oprogramowania (m.in. wirusów ransomware). W tym celu możemy wykorzystać specjalistyczne oprogramowanie w wersji darmowej m.in. *Veeam* Backup & Replication for Windows Free, rozwiązania chmurowe (OneDrive, Google Drive) oraz zewnętrzne nośniki danych.

19. Plik z danymi poufnymi lub osobowymi wysyłany mailem powinien być zaszyfrowany – można wykorzystać darmowego 7-ZIP i odpowiednio skomplikowanego hasła. Nie jest to zabezpieczenie idealne. Pamiętaj, że każde hasło można złamać. Potrzebny jest do tego czas oraz odpowiednia moc obliczeniowa. Jeżeli Twoje hasło będzie długie i skomplikowane nikomu nie będzie się opłaciło sprawdzanie, co wysłałeś pocztą.

Podczas wysyłki maila należy zwrócić uwagę czy wybrany adresat jest właściwy. Nie należy wysyłać informacji do grupy adresowej jeżeli spowoduje to, że poszczególni odbiorcy będą widzieć swoje adresy e-mail. Adres poczty elektronicznej to również chronione dane osobowe. Należy przed wysyłką poczty wykorzystać opcję kopii ukrytej w aplikacji pocztowej.



20. Nie otwieraj żadnych podejrzanych linków znajdujących się w treści otrzymanego maila lub załączników których się nie spodziewamy – ryzyko wyłudzenia informacji lub zainfekowania wirusem!
21. Nie ulegaj presji psychicznej (negatywnej lub pozytywnej), jaką próbuje na Ciebie wywrzeć nadawca wiadomości pocztowej – może to być atak phishingowy. Lepiej zanim cokolwiek zrobisz skonsultuj to ze specjalistą ds. bezpieczeństwa internetowego lub znajomym informatykiem, który pomoże Ci zidentyfikować źródło wiadomości. Jeżeli jednak nie masz pod ręką nikogo takiego zadzwoń do instytucji, która prosi Cię w mailu lub SMS-ie o wykonanie określonej czynności. Pamiętaj aby numer telefonu wziąć nie ze stopki wiadomości ale z innego źródła (ulotki, umowy, strony której adres wpisałeś samodzielnie a nie przeklinałeś w treści podejrzanej wiadomości – to BARDZO WAŻNE).
22. Pamiętaj, że adres, z którego otrzymujesz wiadomość e-mail można idealnie podrobić i podszyć się pod dowolny podmiot (taki jak bank) czy instytucję (np. Urząd Skarbowy). Sprawdzaj skąd faktycznie przyszła wiadomość odpowiadając na maile a przed klinknięciem w link zawsze upewnij się, czy prowadzi do tego miejsca, co powinien (np. na stronę logowania banku).
23. Pamiętaj, że phishing polega również na wykorzystaniu przez przestępców innych kanałów komunikacji takich jak SMS-y, strony internetowe, czy komunikatory.
24. W Internecie znajdziesz dużo informacji związanych ze sposobami obrony przez phishingiem. Pamiętaj, że przed tego rodzaju atakiem nie obroni Cię żaden system antywirusowy czy inny element bezpieczeństwa (częściowo takie wiadomości są odsiewane przez firmowe filtry antyspamowe). W tego rodzaju zagrożeniach technologie obronne oparte na mechanizmach sztucznej inteligencji często zawodzą. Najlepszym obrońcom jest nasza samoświadomość, co do wagi i konsekwencji zagrożenia.
25. Jeżeli Twoje dane zostały zaszyfrowane w wyniku działania wirusa typu ransomware to nie czekaj, działaj. Na stronach Ministerstwa Cyfryzacji znajdziemy szczegółowe porady w tym zakresie.

https://www.gov.pl/web/baza-wiedzy/cyberbezpieczny-samorzad