Getin Noble Bank S.A.
ul. Przyokopowa 33
01-208 Warszawa
Infolinia +48 (22) 203 03 01
Internet www.noblebank.pl

Co to jest "Phishing"?

Phishing jest metodą wykradania poufnych danych przez przestępców w Internecie i dotyczy między innymi Klientów banków. Termin tłumaczy się jako password harvesting fishing, czyli łowienie haseł.

Przestępcy podszywają się pod osoby prywatne lub instytucje i kontaktują się z wybraną grupą użytkowników za pomocą specjalnie spreparowanych wiadomości e-mail lub w komunikatorach internetowych. Komunikaty takie nie wzbudzają na pierwszy rzut oka wątpliwości, ponieważ do złudzenia przypominają te przesyłane przez instytucje: posiadają podobną szatę graficzną, logo itp. W wiadomościach, które wyglądają na autentyczne podają fałszywe informacje np. o wygasającym haśle, zmianach w regulaminie, zmianie danych itp. W wiadomości znajduje się też link, który ma prowadzić do rozwiązania powyższej sytuacji, a faktycznie prowadzi do fałszywej strony logowania do bankowości.

Nieświadomy użytkownik wpisuje swoje poufne dane od logowania, które trafiają do bazy danych przestępców. Dodatkowo żeby to zatuszować pojawia się komunikat, że wszystko jest podane poprawnie.

Ofiarą phishingu można również paść, robiąc zakupy w sklepie internetowym i podając w nim swoje dane przy dokonywaniu płatności. Również wtedy podane przez użytkownika dane nie trafiają do odpowiedniej instytucji czy sklepu, lecz do bazy danych przestępców.

Należy zatem przykładać szczególną uwagę do treści otrzymywanych wiadomości i zawsze przed podaniem swoich danych sprawdzić poprawność adresu strony oraz certyfikatu szyfrowania strony (po kliknięciu w kłódkę na pasku adresu). Wszystkie podejrzane wiadomości należy niezwłocznie zgłosić do banku. Szczegóły dotyczące bezpiecznego logowania do Bankowości Internetowej można przeczytać na tej stronie.

JAK CHRONIĆ SIĘ PRZED PHISHINGIEM?

1. Należy zwróć szczególną uwagę na wiadomości zawierające prośbę o podanie danych osobowych, finansowych, w których nadawca prosi o pilne zalogowanie się czy wypełnienie formularza. Jeśli jakaś wiadomość wzbudza podejrzenia, nie należy klikać w linki w niej zawarte i niezwłocznie ją usuń.

2. W przypadku przekierowania na stronę logowania instytucji wyglądającej podobnie do strony codziennego logowania, należy sprawdzić czy adres strony jest prawidłowy - często może różnić się jedną literą lub znakiem.

3. Podczas dokonywania zakupów po raz pierwszy w sklepie internetowym warto sprawdzić dane kontaktowe właściciela sklepu, poszukać opinii na jego temat. Jeśli strona wzbudzi podejrzenia, najlepiej wycofać się z zakupów w tym sklepie.

4. Podczas dokonywania zakupów w Internecie należy upewnić się, czy przeglądarka nie wyświetla komunikatu o tym, że strona na którą wchodzimy jest podejrzana. Warto sprawdź, czy w adresie strony znajduje się informacja o protokole https, czy widoczna jest kłódka, a po kliknięciu w nią wyświetlane są informacje na temat certyfikatu.