

Description du phénomène / mode opératoire	Augmenter votre sécurité
<p>Escroquerie au Président ("Social engineering")</p> <p>Sur le front des phénomènes criminels sériels au préjudice des entreprises, après une période d'accalmie, la Police neuchâteloise constate une nette reprise des tentatives d'escroqueries appelées « Escroquerie au Président ».</p> <p>Technique de l'escroquerie :</p> <p>Après avoir fait des recherches sur la future victime, notamment au travers d'Internet ou par des appels téléphoniques invoquant diverses raisons et prétextes, le modus operandi consiste à contacter un employé de la comptabilité par un premier courriel envoyé de son soi-disant directeur de l'entreprise (usurpateur) demandant s'il avait déjà été contacté par un pseudo avocat.</p> <p>Dans la foulée, le pseudo avocat appelle cet employé. S'en suit de multiples courriels, provenant des pseudos directeur et avocat, exigeant de la part de l'employé une confidentialité totale, sous le prétexte d'une offre publique d'achat ou d'un contrôle fiscal. Le pseudo directeur exige également que tous les échanges se fassent par courriel. De fil en aiguille, l'employé est amené à établir de multiples ordres de paiement en dérogeant aux règles usuelles, sous les prétextes de l'urgence et de la confidentialité.</p> <p>Les auteurs sont établis ou utilisent des comptes bancaires, notamment en Israël, France, Chine et Chypre.</p> <p>Des variations de la mise en scène peuvent intervenir, les escrocs faisant preuve d'une grande faculté d'adaptation.</p>	<p>Mesures préventives:</p> <ul style="list-style-type: none">- informer le personnel de l'entreprise de ce type d'escroquerie,- ne jamais utiliser le bouton "répondre" des courriels, mais systématiquement en rédiger un nouveau, l'adresse électronique des auteurs étant une "contrefaçon" visuellement proche de l'original,- prendre contact téléphoniquement ou "de visu" avec le directeur,- ne jamais agir dans l'urgence (sous la pression de tierces personnes),- ne pas contrevenir aux règles usuelles de sécurité interne à l'entreprise (sous le couvert de l'urgence et de la confidentialité),- inventorier les informations et documents éventuellement fournis aux auteurs par mégarde et étudier les suites à donner avec l'inspecteur de la brigade de cyber enquêtes,- en cas de doutes, contacter l'inspecteur de la brigade de cyber enquêtes (tél. 032/889.90.00).