



AUSTRALIAN COMPETITION
& CONSUMER COMMISSION

코로나19 (코로나바이러스) 관련 발생 피싱사기

2020년 6월

코로나19 (코로나바이러스) 팬데믹을 이용한 사기범들의 사기행위가 호주 전국에 발생중입니다. 피싱사기는 현재 3가지 유형의 사례가 주로 사용되고 있습니다.

피싱을 이용한 개인정보 편취

사기범들이 유명 기업이나 정부기관을 사칭하는 전화나 이메일, 문자 연락을 통해 코로나19 정보나 서비스 안내 명목으로 웹링크 접속이나 소프트웨어 다운로드를 유도하여 피해자의 개인정보를 편취하는 방식 (피싱).

연금(Superannuation) 사기

코로나19의 영향으로 재정적으로 어려운 피해자에게 접근하여 연금을 탈취하거나 불필요한 서비스 가입을 유도하여 수수료를 갈취하는 방식

연금회사나 금융업체 직원을 사칭하여 다음과 같은 방법으로 피해자의 연금 계정관련 정보를 알아내는 사기방식입니다:

- 연금의 조기환급 절차를 도와준다는 제의를 하거나.
- 코로나19 로 새로 법규가 바뀌었다며 슈퍼연금 계정이 잠금되지 않도록 도와준다고 하거나.
- 피해자의 계정이 다양한 혜택의 수혜요건에 부합되는지 확인해 주겠다고 하는 방식.

온라인쇼핑 사기

유령 온라인 쇼핑몰을 오픈하여 코로나19 치료제, 백신 등 허위성 제품이나 마스크 등 희귀상품을 판매한다고 광고하는 방식.

피싱사기 피해 방지법

- 신뢰할 수 있는 기관에서 온 문자나 SNS, 이메일로 보이더라도 포함된 링크를 클릭하여 접속하면 안됩니다.
- 홈페이지 연결은 새 인터넷 창에서 직접 주소를 입력하여 접속하십시오. 예를 들어서 마이가브(MyGov) 사이트에 접속하려면, 검색창에 my.gov.au를 직접 입력하여 연결합니다.
- 유명업체나 정부기관에서 온 전화나 문자더라도 개인정보나 재정금융정보를 요구할 경우에는 답하지 말고 통화를 끊거나 문자를 삭제하십시오.
- 전자상거래 사기와 온라인쇼핑 사기를 판별하기 위한 최선의 방법으로는 구매 이전에 사용자후기를 검색해볼 수 있습니다. 현재까지 코로나19 치료제와 백신은 없습니다.
- 우체국 송금수표, 온라인 이체, 국제송금, 선불카드, 비트코인을 포함한 전자화폐 등 비통상적 방식으로 선지급 결제를 요구하는 판매업자는 의심해보시기 바랍니다.

주의: 조금이라도 수상할 경우 절대로 진행하지 마십시오.

사기 관련 더 자세한 정보는 [스캠워치\(Scamwatch\)](#) 홈페이지에 [신고방법](#)과 [도움요청방법](#) 정보 등이 포함되어 안내되어 있습니다.