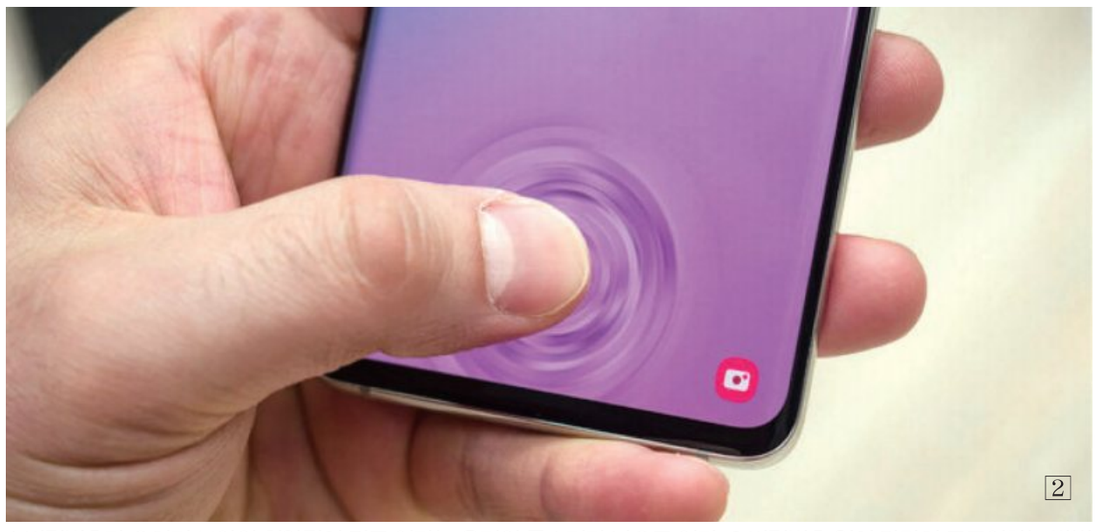
FOCUS

비밀번호 없는 세상이 온다고?

한세희 IT 칼럼리스트

2020년 유출된 인텔 기밀 파일 패스워드, 알고 보니'intel123'

애플·구글·MS, FIDO와 손잡아 표준기술의 개인 암호화 키 유력



1 비밀번호가 오히려 보안의 취약점이 되고 있다는 우려의 목소리가 나오고 있다. 2 비밀번호 없이 간단히 로그인하는 방법으로 스마트폰에서는 지문 인식이나 얼굴 인식 기술을 사용하고 있다. 〈중앙포토〉

인터넷은 일상의 많은 일을 점점 간편하고 편리하게 만들고 있다. 하지만 반대로 온라인에서 갈수록 어렵고 복잡해지는 일이 있다. 바로 비밀번호 만들기다. 요즘 인터넷 서비스나 앱에 신규 가입하려면 영문 대소문자와 숫자, 특수문자가 섞인 최소 열 자리 이상의 비밀번호를 만들어야 한다. 생일이나 이름과 관련된 글자나 숫자도 안 된다. 비밀번호를 정기적으로 바꾸라며 귀찮은 메시지가 계속 뜬다. 물론 비밀번호를 'Ec0#03nO94*&miSt0jH%' 같이 만들면 계정은 거의 절대적으로 안전하다. 하지만 이런 비밀번호를 외우고 다닐 수는 없다. 시스템의 요구에 따라 복잡한 비밀번호를 만들고, 이를 잊지 않으려 수첩에 적거나 심지어 포스트잇에 적어 모니터에 붙여 놓는 웃지 못할 일도 생긴다.

보통 적당히 강력한 비밀번호를 하나 만들어 모든 사이트에 똑같이 쓰곤 한다. 자신만의 어구와 변형 규칙을 만들어 이를 여러 사이트에 적용하는 것은 그래도 보안에 신경을 쓰는 경우다. LG트윈스 팬이라 'LGTw1ns'라는 문구를 고정적으로 넣고, 구글 비밀번호는 'LGTw1nsGoogle', 신한은행 앱 비밀번호는 'LGTw1nsShinh@n'으로 짓는 식이다. 이렇게 암호를 만든 사람은 아마 기억하기 좋은 규칙성과 해킹하기 어려운 복잡성 사이의 균형을 잡았다고 생각할 것이다. 그렇지 않다. 사람들이 생각하는 패턴은 거의 비슷하다. 사용자에 대한 몇 가지 힌트를 조합하면 많은 경우 어렵지 않게 비밀번호를 추정할 수 있다. 한 곳을 뚫으면 비슷한 변형 규칙을 시도해 다른 사이트 계정도 모두 털 수 있다.

사용자에 대한 힌트를 찾기는 그리 어렵지 않다. 우리는 소셜미디어에 생일이나 위치, 가족, 좋아하는 것들에 대한 흔적을 수없이 남긴다. 키보드 입력을 가로채는 소프트웨어는 어둠의 경로로 쉽게 구할 수 있다. 피싱 문자는 끊임없이 날아온다. 스마트폰 잠금 화면에 넣는 핀 번호를 누군가 어깨 너머로 보고 있을지도 모른다. 영화와 달리 대부분의 해킹은 네이버나 농협의 시스템 허점을 공격하는 방식으로 이뤄지지 않는다. 대략 80%의 해킹은 나의 로그인 정보를 누군가 가로챘기 때문에 일어난다.

개인정보와 금융정보, 민감한 사진과 메시지가 모두 스마트폰과 인터넷 클라우드에 있으니 강력한 비밀번호로 문을 굳게 지키란 충고는 적절해 보인다. 하지만 사람의 인지 능력엔 한계가 있다. 집에 들어갈 때마다 12개의 자물쇠를 열 수는 없는 노릇이다. 해킹 피해는 아직 일어나지 않았고 나에게 실제 닥칠지도 알 수 없지만, 지금 복잡한 비밀번호를 입력하는 것은 귀찮다. 그래서 정보보호 전문가들이 아무리 외쳐도 비밀번호 문제는 좀처럼 나아지지 않는다. 2020년 인텔의 기밀 파일이 유출되는 사건이 있었는데, 문제의 파일에 걸린 비밀번호는 'intel123'이었다.

따지고 보면 인터넷 개인정보에 대한 주요 공격 채널 중 하나가 바로 비밀번호다. 보안을 지키려 만든 비밀번호가 보안 취약점이 되어버렸다. 쉽게 떠오르는 해결책은 비밀번호를 더 복잡하게 만드는 것이다. 하지만 발상을 바꿔 비밀번호가 필요 없게 만들면 어떨까? 비밀번호 없이 간단히 로그인하게 하는 시도는 계속 이뤄지고 있다. 요즘 스마트폰에서 흔히 볼 수 있는 지문 인식이나, 얼굴을 인식해 잠금을 해제하는 아이폰 페이스ID가 대표적이다. 생체 정보를 활용하면 로그인의 비밀번호 허들을 상당히 낮출 수 있다. 하지만 아직 모바일 기기와 PC, 앱과 웹사이트 등 사용자가 접하는 모든 디지털 환경에서 공통적으로 비밀번호 없이 활동하게 할 수는 없다.

앞으로는 그렇게 될지도 모르겠다. 최근 애플과 구글, 마이크로소프트가 완전히 비밀번호가 없는 세상을 만들기 위해 협력한다고 밝혔다. 이를 위해 비밀번호 없이도 편리하게 사용자를 인증하는 기술과 표준을 만드는 업계 단체 FIDO와 손잡았다. 이들이 만드는 스마트폰과 PC 운영체계(OS), 인터넷 브라우저, 메일과 계정 서비스는 세계 대부분의 사람이 쓴다. 비밀번호 없는 환경을 만드는 데 가장 크게 기여할 수 있는 기업들이다. FIDO의 표준 기술로 만든 개인 암호화 키를 사용자 기기에, 공개 암호화 키를 웹서비스에 두어 사용자가 스마트폰을 잠금 해제하면 PC에서 접속한 사이트에 곧바로 로그인이 되게 하는 방식 등이 유력하다. 스마트폰 잠금 해제가 양측의 암호화 키를 확인하는 역할을 하는 것이다. 기기나 OS, 브라우저 종류에 상관없이 작동하게 한다는 목표다.

기존 비밀번호 없는 로그인은 적어도 처음 한번은 비밀번호를 입력해야 하는 반면, 앞으로는 이런 과정도 없앤다는 것이다. 사용자 기기와 사이트가 서로 키를 확인해야 하므로 실제 사이트와 똑같은 가짜 사이트를 만들어 비밀번호 입력을 유도하는 피싱도 막을 수 있다. 가짜 사이트는 암호화 키를 갖고 있지 않기 때문이다. 비밀번호 없이도 오히려 더 안전하고 편리한 인터넷 환경을 만든다는 큰 그림이다. 이는 사용자는 물론, 기업들에게도 좋은 일이다. 비밀번호를 입력하거나, 기억하지 못해 다시 찾는 과정에서 적지 않은 사용자가 이탈하기 때문이다.

물론 비밀번호 없는 인터넷 환경을 위한 기술과 서비스가 완성되기까지는 아직 시간이 필요하다. 그때까지는 강력한 비밀번호로 스스로 정보를 지켜야 한다. 비밀번호는 길수록 안전하다.

16자리 이상이 좋다. 여러 사이트 비밀번호에 공통 어구를 쓰고 싶다면, 본인에게만 의미 있고 다른 사람에게는 일반적으로 보이는 단어를 조합하는 것이 좋다. 생일도 피해야 한다. 특수문자를 넣기 위해 a를 @으로, 1을 !로 대체하는 트릭도 모든 해커가 알고 있다. 소셜미디어에 개인정보를 유추할 만한 내용은 최소화한다. OTP 같은 2단계 인증도 추천한다. 로그인 후 스마트폰 앱이나 문자로 날아온 일회용 코드를 한번 더 입력하는 방식이다. 각 사이트마다 임의의 길고 복잡한 비밀번호를 만들어주는 패스워드 매니저 앱을 쓰는 것도 좋은 방법이다. 이런 방법들이 해킹 위험을 완전히 없앤다고 장담할 수는 없지만, 위험을 현저히 줄이는 것은 사실이다. 고백하자면, 여기 소개한 대부분의 주의 사항은 나도 잘 지키지 못하고 있다. 어서 비밀번호 없는 세상이 오기를 기다리는 이유다.

〈광주일보와 중앙 SUNDAY 제휴 기사입니다〉