



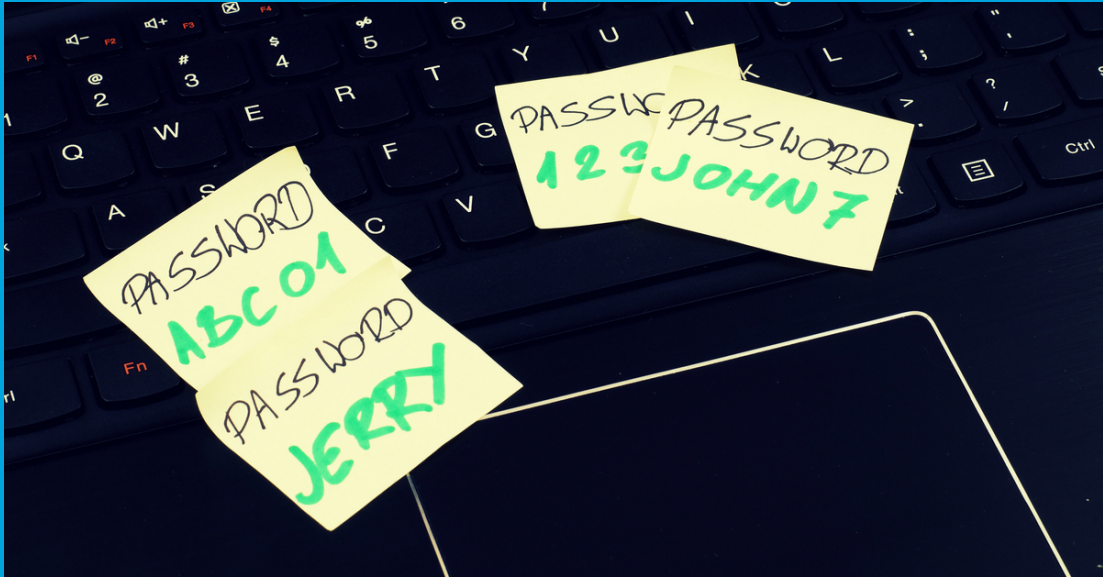
---

# Security Newsletter

26 November 2018

[Subscribe to this newsletter](#)

# The passwordless web explained



On 20 November 2018, Microsoft announced that its 800 million Microsoft account holders could now log in to services like Outlook, Office, Skype and Xbox Live without using a password. The announcement is part of an apparent acceleration in the march towards a passwordless web, and comes at the end of a year when Mozilla Firefox, Google Chrome and Microsoft Edge all rolled out support for WebAuthn, one of the keystone technologies.

Passwordless authentication means ditching usernames and passwords in favour of biometrics, like fingerprints and face recognition, or other forms of authentication compatible with the FIDO2 specification, such as YubiKeys or Titans.

One of the reasons that passwords have hung around for so long is that they're very, very easy to understand. Passwordless authentication works in a different way, isn't as easy to grasp, and comes with a lexicon of new (or relatively new) acronyms and standards like FIDO2, WebAuthn and CTAP. Passwordless authentication is a Good Thing and it deserves some explanation. In this article I'll try to explain, in simple terms, how it all works, what some of the important acronyms mean and how they fit together.

[Read More on Sophos NakedSecurity blog](#)

## More #News

- [How a Security Test for DropBox Revealed 3 Apple Zero Day Vulnerabilities](#)
- [AWS rolls out new security feature to prevent accidental S3 data leaks](#)
- [CarsBlues Bluetooth Hack Allows Hackers to Access Text Messages, Call Logs and More](#)
- [Tesla Gave Me Control Of Their Site Forums](#)
- [Leaderboard Shows Adoption of DMARC Email Security Protocol](#)
- [USPS Site Exposed Data on 60 Million Users](#)
- [Magecart group hilariously sabotages competitor](#)
- [Edge Browser Can Now Sign Into Microsoft Accounts With FIDO2 Security Keys](#)
- [Mobile and IoT attacks – SophosLabs 2019 Threat Report](#)
- [First GDPR Sanction in Germany Fines Flirty Chat Platform EUR 20,000](#)
- [Hacker says USPS ignored serious security flaw for over a year](#)
- [Rowhammer attacks can now bypass ECC memory protections](#)
- [German e-government SDK patched against ID spoofing vulnerability](#)
- [Amazon data breach: Names & email addresses of customers exposed online](#)

## #Patch Time!

- [Patch Skype for Business now or risk DoS via emoji kittens!](#)
- [Apache Hadoop spins cracking code injection vulnerability YARN](#)
- [VMware Releases Critical Security Updates for Multiple Vulnerabilities](#)

## #Tech and #Tools

- [Practical Cryptography for Developers - Free Book](#)
- [S3Inspector: Check for public S3 buckets](#)
- [SaSSHimi: evading AllowTcpForwarding](#)
- [Password Strength Meter Comparison](#)
- [How Azure AD Could Be Vulnerable to Brute-Force and DOS Attacks](#)
- [Web Browser Address Bar Spoofing](#)
- [Faking the German government-issued identity card online](#)
- [Yet another memory leak in ImageMagick or how to exploit CVE-2018-16323.](#)
- [Active Directory Kill Chain Attack & Defense](#)
- [Awesome Windows Domain Hardening](#)
- [Windows 10 Security Checklist Starter Kit](#)



This content was created by [Kindred Group Security](#). Please share if you enjoyed!

## Kindred Group in brief

Kindred is one of the largest online gambling companies in the world with over 24 million customers across 100 markets. We offer pre-game and live Sports betting, Poker, Casino and Games through 11 brands across our markets. We are committed to offer our customers the best deal and user experience possible, while ensuring a safe and fair gambling environment. Kindred is a pioneer in the online gambling industry and as an innovation driven company that builds on trust.

You can access the previous newsletters at <https://news.infosecgur.us>