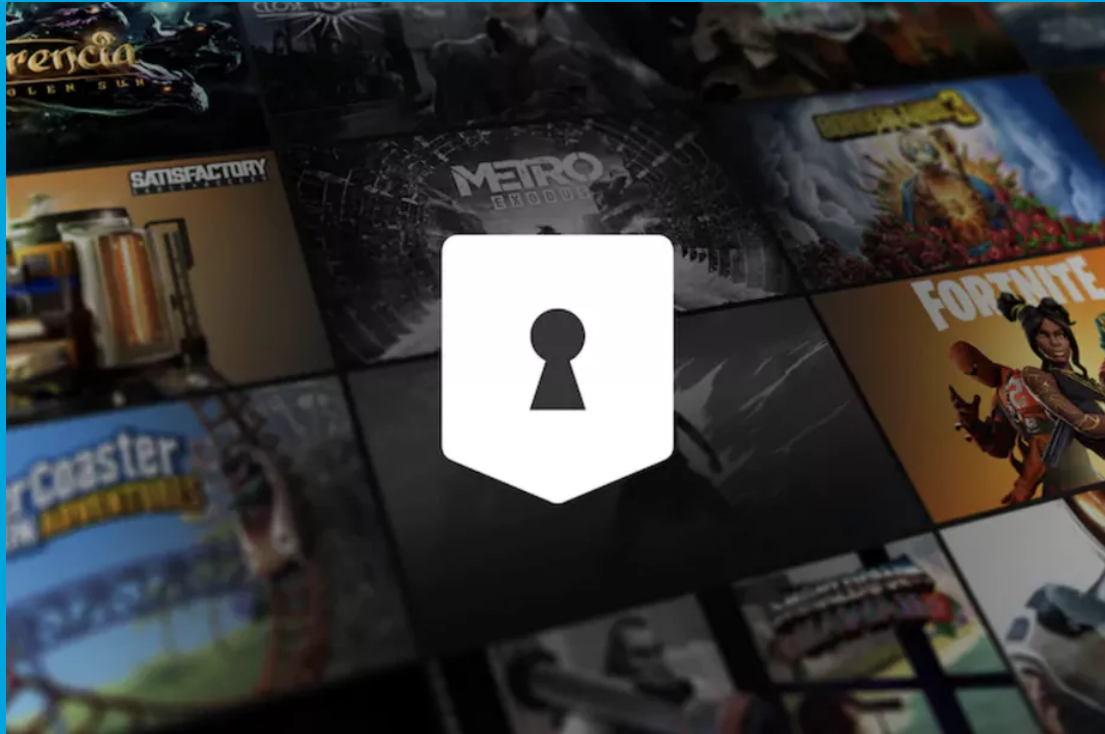# Security Newsletter

4 May 2019

Subscribe to this newsletter

Epic Games is requiring customers to enable two-factor authentication to redeem free games

Epic Games will occasionally require users to enable two-factor authentication before redeeming free games on its digital storefront between now and May 21st. The goal is to encourage "players to take steps to strengthen their Epic account security," the company wrote in a blog post. To enable two-factor authentication, users have to log into the Epic Games Store and head into their account settings.

In January 2019, a security flaw in Fortnite allowed hackers to access the Epic Games accounts of users who clicked a suspicious link. A few days ago, Nintendo acknowledged that 160,000 Nintendo accounts were impacted in hacking attempts, which started earlier this month. Nintendo urged all of its users to activate 2FA on their Nintendo accounts, which proved to be an effective block against the exploit that targeted the dated Nintendo Network (NNID) account system.

Read More on TheVerge

Official statement from Epic Game

More #News

- Google discloses zero-click bugs impacting several Apple operating systems
- New Firefox service will generate unique email aliases to enter in online forms
- Latest Phishing Campaign Spoofs Microsoft Teams Messages
- New Android malware steals financial information, bypasses 2FA
- Hacker sells 91 million Tokopedia accounts, cracked passwords shared
- French daily Le Figaro database exposes users' personal info
- Ninja Forms WordPress bug exposed over a million users to XSS attacks, website hijacking
- CursedChrome turns your browser into a hacker's proxy
- Numerous sites leak user emails to advertising, analytics services

#Patch Time!

- Critical Bugs Found in 3 Popular e-Learning Plugins for WordPress Sites
- Several Vulnerabilities Patched With Release of WordPress 5.4.1
- Adobe patches critical code, corruption bugs across Bridge, Illustrator, Magento

#Tech and #Tools

- Honeysploit: Exploiting the Exploiters
- Microsoft releases Sysmon 11 with auto-backup of deleted files
- Staying Off the Land: A Threat Actor Methodology
- OSCP After Marriage!
- AWS Defender Track
- Splunk Attack Range in a virtualized Ubuntu Guest VM — Guide
- Excelerating Analysis – Tips and Tricks to Analyze Data with Microsoft Excel
- Beware of the GIF: Account Takeover Vulnerability in Microsoft Teams
- Mute Sysmon - Silence Sysmon via event manifest tampering
- Tutorial: Creating a custom full featured implant
- Cyber OSINT CTF (Event)
- Guy's 30 Reverse Engineering Tips & Tricks
- Zero Dollar CTF Infrastructure.
- SOPS: Simple and flexible tool for managing secrets
- Finding evil in AWS: A key pair to remember

Kingred Group is growing, so does the Group Security team! We're looking for new talented professionals to come join us:

- You like to break things, then explain how to fix it? Be part of our Cyber Security team
- You prefer the blue team side? Check out our Security analyst position
- Interested in Governance, Risk and Compliance? Apply for our Information Security Specialist role

Kindred is one of the largest online gambling companies in the world with over 24 million customers across 100 markets. You can find all our open vacancies on our career page.

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