STRIKEREADY

Dark Web Report

namal.edu.pk.

Time Period: 09/02/2025 - 12/02/2025 | Report Date: 12-02-2025

Overview

Dark web monitoring conducted over the last three months identified 11 exposed credentials associated with the domain *namal.edu.pk*. Microsoft Entra ID validation confirms 5 credentials are linked to active accounts, while 6 are associated with inactive accounts. The identity *abdullah2018@namal.edu.pk* has the most exposure. Among all exposed credentials, the most frequently observed password is *"campus@123"*.

Exposure Details

11 Total Exposed Credentials

05 Active accounts

06 Inactive accounts

02 Passwords older than a year

04 Passwords older than two years

05 Passwords older than four years

Total Exposed Credentials

URL	User	Password	Breach Date	StealerMalware
https://www.facebook.com/	abdullah2018@namal.edu.pk	******	11-03-2025	-
https://www.amazon.com/	abdullah2018@namal.edu.pk	******	11-03-2025	-
https://www.google.com/	abdullah2018@namal.edu.pk	******	11-03-2025	-
https://www.facebook.com/	abdullah2018@namal.edu.pk	******	11-03-2025	-
https://www.facebook.com/	abdullah2018@namal.edu.pk	******	11-03-2025	-
https://www.facebook.com/	abdullah2018@namal.edu.pk	******	11-03-2025	-
https://www.facebook.com/	abdullah2018@namal.edu.pk	******	11-03-2025	-
https://www.facebook.com/	abdullah2018@namal.edu.pk	******	11-03-2025	-
https://www.facebook.com/	abdullah2018@namal.edu.pk	******	11-03-2025	-
https://www.facebook.com/	abdullah2018@namal.edu.pk	******	11-03-2025	-
https://www.facebook.com/	abdullah2018@namal.edu.pk	******	11-03-2025	-

Active Accounts

URL	User	Password	Breach Date	StealerMalware
https://www.facebook.com/	abdullah2018@namal.edu.pk	******	11-03-2025	-
https://www.facebook.com/	abdullah2018@namal.edu.pk	******	11-03-2025	-
https://www.facebook.com/	abdullah2018@namal.edu.pk	******	11-03-2025	-
https://www.facebook.com/	abdullah2018@namal.edu.pk	******	11-03-2025	-
https://www.facebook.com/	abdullah2018@namal.edu.pk	******	11-03-2025	-

Microsoft Entra ID Validation

- Microsoft Entra ID confirmed credentials status.
- Active accounts flagged for immediate remediation.
- Inactive accounts marked for credentials reuse and monitoring.

Recommended Actions

- Immediate password reset for all active compromised accounts.
- Ensure MFA enforcement for affected users and all users across the domain.
- Kill all active sessions linked to exposed accounts.
- Temporarily disable users exhibiting suspicious behavior until secured.
- Remove unnecessary privileges from all compromised accounts.
- Track any attempts to reuse the inactive compromised credentials.
- Monitor external-facing services for suspicious login attempts.
- Conduct credential-hygiene and phishing awareness training to reduce password reuse and limit compromise risk.

Conclusion

Immediate remediation is required for all exposed credentials to prevent unauthorized access. Implement password resets, enforce MFA, maintain continuous monitoring, and conduct awareness training for all users to reduce the risk of future compromise and ensure account security.