23andMe October 2023 Credential Stuffing Attack

Incident Name	23andMe October 2023 Credential Stuffing Attack
Date of Incident	2nd October 2023
Summary	23andMe is a biotechnology company based in California. They provide genetic testing to customers, offering details on their ancestors and genetic health data. On October 2, 2023, records claiming to be breached from 23andMe appeared on a popular breach forum. A sample of data was made available, and a few days later, more 23andMe profile data was offered for sale in bulk. The data includes names, dates of birth, genetic ancestry results, and geographical locations. On October 6th, 2023, 23andMe publicly acknowledged the breach and released details in a blog post. They stated that they were investigating the breach and asking customers to reset their passwords while encouraging the use of MFA on their accounts. They believe customer accounts were breached by threat actors who used compromised login credentials from other services in a credential stuffing attack. They are advising customers to ensure they use unique passwords for all their accounts to prevent password reuse.
Key Social Engineering/OSINT Themes	• **Recon** - Harvesting emails and password data from previous breaches. • **Credential Stuffing** - Using breached login credentials, the threat actor was able to access a number of accounts where customers reused passwords and MFA was not enabled.

Picnic's Recommended Remediations.
 	
For detailed remediations, see the Human Attack Surface Protection Framework (HASP).
	High Risk Employees
	• **HASP Framework 1.1 — Identify high value employee targets**
	  ◦ MITRE Alignment: T1589
	  ◦ NIST CSF Alignment: ID.RA-1
	• **HASP Framework 1.3 — Conduct social engineering risk assessments for high value employee targets**
	  ◦ MITRE Alignment: M1047
	  ◦ NIST CSF Alignment: ID.RA-5
	• **HASP Framework 1.5 — Establish and implement procedures for high value employee targets**
	  ◦ MITRE Alignment: M1056

	- NIST CSF Alignment: PR.IP-7 **HASP Framework 1.7 — Increase detection and monitoring for high value employee targets** - MITRE Alignment: M1040 - NIST CSF Alignment: DE.CM-3 Exposed Employee PII **HASP Framework 2.1 — Identify exposed employee PII** - MITRE Alignment: T1589 - NIST CSF Alignment: ID.RA-2 **HASP Framework 2.2 — Reduce exposed employee PII** - MITRE Alignment: M1056 - NIST CSF Alignment: PR.IP-7 Exposed Credentials **HASP Framework 3.1 — Identify exposed work credentials** - MITRE Alignment: T1589.001 - NIST CSF Alignment: ID.RA-2 **HASP Framework 3.2 — Identify exposed personal credentials** - MITRE Alignment: T1589.001 - NIST CSF Alignment: ID.RA-2 **HASP Framework 3.4 — Empower employees to mitigate risk through credential management** - MITRE Alignment: M1027 - NIST CSF Alignment: PR.AC-1 **HASP Framework 3.5 — Reset passwords of currently-set exposed credentials** - MITRE Alignment: M1027 - NIST CSF Alignment: PR.AC-1 **HASP Framework 3.6 — Block work, personal, and service exposed credentials from reuse** - MITRE Alignment: M1027 - NIST CSF Alignment: PR.AC-1 **HASP Framework 3.8 — Monitor for account takeover (including real time alerts on exposed credentials)** - MITRE Alignment: DS0028 - NIST CSF Alignment: DE.CM-3
Industry	Biotechnology
Actor	Unknown
Motivations	Financial
Related Industry Hacks	MediBank, Henry Ford Health, HCA, MCNA Dental, McLaren Health Care
Breach Notice/Company	23andMe Blog: Addressing Data Security Concerns

Notice	
Other Sources	• Bleeping Computer: Genetics firm 23andMe says user data stolen in credential stuffing attack • Cybersecurity Insiders: Credential stuffing cyber attack leads to data breach of genetic info of Jewish Community • Wired: 23andMe User Data Stolen in Targeted Attack on Ashkenazi Jews