Threat Actors Impersonate ParentSquare in Phishing and Social Engineering Attacks

***Author**: Portia S. Cole – CTI Researcher*

TL;DR

Threat actors are impersonating ParentSquare in phishing and social engineering attacks targeting K-12 school communities.

Most activity involves phishing emails using DocuSign branding and electronic signature requests.

Overview

Threat actors are using ParentSquare as a phishing lure to target parents, teachers, school staff, and students. ParentSquare is a communication platform (an app) used by K-12 school districts to send routine school communications. Because these messages are expected, recipients may be less likely to question phishing emails that appear to come from the platform.

Affected Products:

- ParentSquare
- ParentSquare Mobile Application
- ParentSquare Email Communications
- DocuSign-branded phishing lures (impersonation only)

ParentSquare-related phishing and impersonation activity dates back to at least the beginning of the 2025-2026 school year, when parents began reporting suspicious ParentSquare account activity and impersonation attempts. Since then, multiple school districts have warned families about attackers masquerading as ParentSquare and school personnel through several forms of social engineering.

Email phishing is the primary attack method. Observed lures include DocuSign-branded (an e-signature service) electronic signature requests, fake contracts, privacy agreements, and account verification requests that direct recipients to credential harvesting websites.

Voice phishing (vishing) has also been reported. Attackers impersonate school staff over the phone to request payment information. Other observed activity includes fake laptop sales and education-related service offers.

Education organizations are the primary targets because ParentSquare is widely used for routine school communications. So far, the incidents have occured in Virginia and California. No threat actor has been attributed.

Aspire Protects

- Verify ParentSquare messages before clicking links or opening attachments.
    - Hover your mouse over links. Does anything look off?
- Access ParentSquare through the official website or mobile app instead of email links.
- Verify unexpected DocuSign requests with your school before signing documents.
    - Call or email the school directly.
- Inspect sender email addresses and links for misspellings or look-alike domains.
- Never share passwords, MFA codes, payment information, or other sensitive information through email, text messages, or phone calls.
- Report suspected phishing emails, text messages, and phone scams to your IT or security team.

TTPs

Initial Access

- Spearphishing Link (T1566.002) - Threat actors may send phishing emails impersonating ParentSquare and trusted school communications that contain malicious links to credential harvesting website.

Defense Evasion

- Masquerading (T1036) - Threat actors may impersonate ParentSquare, school districts, and DocuSign branding to make phishing emails and electronic signature requests appear legitimate.

Credential Access

- Input Capture: Web Portal Capture (T1056.003) - Threat actors may harvest usernames and passwords through spoofed web portals that imitate legitimate login pages.

IoCs

There are no known IoCs at this time. Aspire is actively monitoring and will notify customers if any are found. For more details on how we can help protect your organization, contact Aspire's Customer Success Management team.

Targeted Industries

ParentSquare phishing and social engineering attacks activity primarily targets organizations in the following sectors:

- Education
  - K-12
  - Public School Districts
  - Charter Schools
  - Private Schools
  - Educational Service Providers

Aspire Service Offerings

- **Aspire Managed XDR (MXDR)**
  - Aspire Managed XDR (MXDR) combines next-generation eXtended Detection and Response (XDR) technology, a 24x7 security operations center (SOC), and the expertise of a US-based team of security professionals to identify and respond to threats across a broader attack surface.
  - Building on the existing capabilities of Managed Detection and Response (MDR), Aspire Managed XDR integrates and correlates telemetry from endpoints, network, cloud, email, identity, and more. This advanced platform creates valuable context enabling end-to-end visibility across all threat vectors.
  - Experienced security analysts and incident responders deliver 24x7 threat detection, analysis, and investigations – with both automated and human-led response actions to quickly mitigate cyber attacks.
- **Aspire Incident Response**
  - The ability to respond effectively to data breaches is critical to every organization. When attacks occur, IT leaders need a process that will ultimately maintain business continuity, protect the company reputation, and avoid fines, legal fees, and remediation costs.
  - Aspire offers incident response services to help you prepare for, manage, and recover from data breaches and network attacks. An experienced team uses industry-leading threat intelligence and the most current security technology to quickly respond to attacks, reduce damage, and minimize exposure.

Supporting Documentation

Fresno Unified warns students and families about potential phone scam - ABC30 Fresno

APS cautions against phishing emails – The H-B Current

VBCPS warns parents about scam involving caller impersonating staff

Concerned Citizens Group for Clinton County, Indiana | Frankfort parent who use parent square check ur page and make sure this didn't happen to you... | Facebook