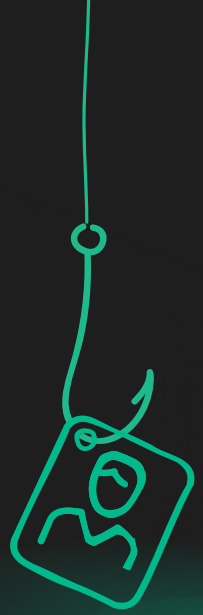
Social Engineering in K-12

for Beginners

jamf



Kids are in school to learn — but not just to learn. School helps them navigate social interactions, build a sense of pride and find validation from peers or others. It's a tumultuous time, not always marked by good judgment.

Attackers know this; that's exactly why they target schools with social engineering attacks.

If they combine urgency and pressure with student naivete, they open a well of nefarious possibilities.

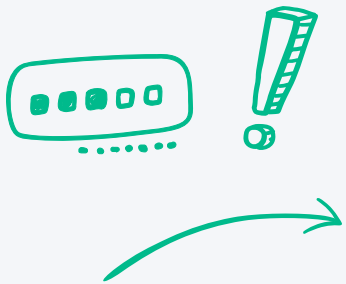
In this e-book, we'll talk about:

- **What social engineering is**
- **Common tactics**
- **How it shows up in K-12 schools**
- **The tools and techniques to prevent attacks**

What is social engineering?

Social engineering uses psychological tactics to trick users into exposing sensitive information. It can be used on its own, like a website made to look like a familiar login page that instead harvests credentials. Or it can work in conjunction with other vectors by delivering malware, for example.

Social engineering targets the human element of your security posture. This is incredibly common, **exceeding other attack vectors by at least 45%**, according to the **2025 CIS MS-ISAC K-12 Cybersecurity Report: Where Education Meets Community Resilience.**



Why does social engineering matter to IT?

In short, it makes your school vulnerable to attacks.
Consider this:

Attackers can circumvent your controls:

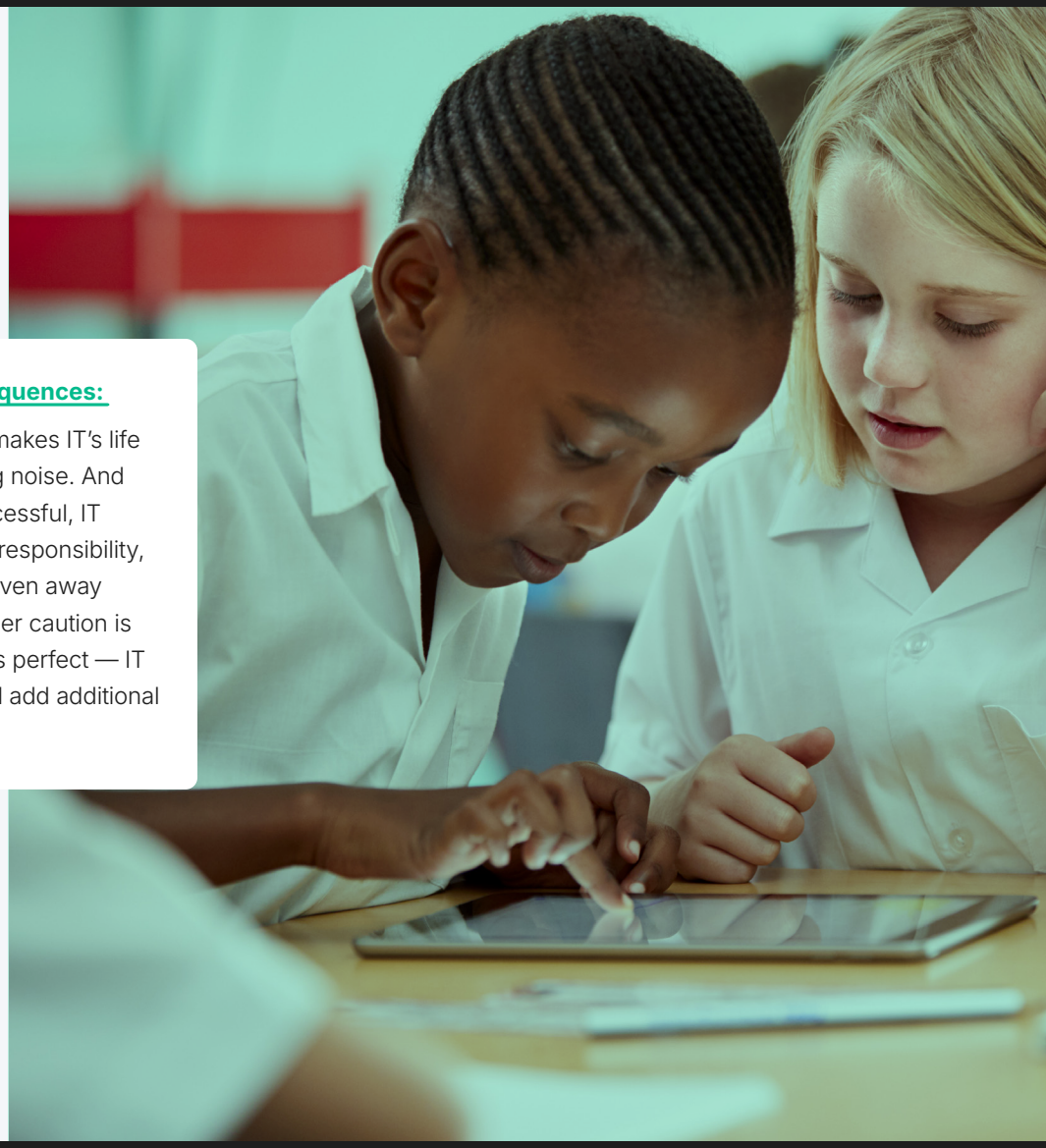
If your IT configurations and safeguards don't address social engineering, they can be bypassed — after all, if the attacker has credentials, their login attempt can appear legitimate without proper tooling.

Lateral movement is a risk:

A single compromised account can open your systems up and increase disruption as attackers can move to more sensitive systems.

IT bears the consequences:

Social engineering makes IT's life harder by increasing noise. And if an attacker is successful, IT bears the weight of responsibility, even if a user has given away their information. User caution is critical, but no one is perfect — IT has to intervene and add additional defenses.



Common social engineering tactics

Phishing

Phishing is a common form of social engineering. Attackers might impersonate school staff or services, mimic legitimate websites and use urgency to get users to give up their information.

Malvertising

Malicious advertising, or malvertising, uses online ads to deceive users into downloading malware or compromise their credentials.

Pretexting

Pretexting can look like a lot of things, but generally it's used to build a user's trust. Attackers may pose as an authority figure or a peer to get users to trust them enough to divulge their information.

Baiting

Baiting lures users in with irresistible propositions: free money, recognition, exclusive content and more. But upon clicking on the link, users install malware or are sent to phishing sites.

SEO poisoning

Attackers take out ads on search engines to put their malicious copycat sites at the top of search results for unsuspecting users to click.

Prompt bombing

Attackers repeatedly send multi-factor authentication requests to annoy a user into granting access.

These techniques have been around for a while. What's new though, is AI's impact. It's totally changing the game. In their **2025 Cost of a Data Breach Report,** IBM found that 1 in 6 data breaches involved AI-driven attacks.

With **generative AI**, attackers can ***"reduce the time needed to craft a convincing phishing email from 16 hours down to only 5 minutes."***

AI results in faster and more convincing phishing attacks and deepfakes — schools need to address these advancements, especially considering the susceptibility of their young users.

How social engineering shows up in K-12 schools

Social engineering shows up in all kinds of cyber attacks. The **Verizon 2025 Data Breach Investigations Report** found social engineering techniques in **17% of attacks on the educational services industry**.

What this actually looks like can vary, since social engineering takes many forms and continues to evolve. Here are some possible scenarios:

Online games? You just got played.

A middle school student is browsing the internet for games after they've completed their assignments. They find themselves on a website advertising free bucks on their favorite online game! They can't resist and click the link, which takes them to a credential-stealing website that promises them virtual wealth — for the cost of their login.

Maybe do look this gift horse in the mouth

Your new teacher is eager to please school administrators. So much so, that when their "principal" sends an email asking for gift card codes, they don't even hesitate. This teacher is too new to recognize that their principal doesn't talk ***quite*** like the email's contents.

True or false: this download is safe
(spoiler: it's false)

A high schooler is preparing to take college entrance exams. They search for test prep resources. The search result on the top of the page is a sponsored link advertising free practice tests. All the student needs to do is download the test prep software, which, surprise, contains malware.

You're gonna be popular... once your data is leaked online.

A group of elementary school students get an email about a school popularity contest — vote for the most popular student and see if you win! We just need to verify that you really are a student at your school; can you provide some personal information?

Stop social engineering in its tracks

So, what can you do to stop social engineering from exploiting your users and threatening your data security? You must approach it from two angles: **your users and your tech stack.**

User education

Your users, especially the younger ones, haven't yet experienced all the good and bad the internet has to offer. Many aren't used to questioning what they see online. Ideally, digital citizenship should be a part of your school's curriculum. Digital citizenship teaches students to use the internet responsibly and safely.

This includes:

- Providing **age-appropriate explanations** about common cyber threats
- Offering **examples** of suspicious websites/ content
- Encouraging ethical and responsible **behavior** online

And of course, your faculty/staff needs training too. Consider:

- Phishing email **simulations**
- Regular, mandated compliance **training**
- Fostering a **culture of transparency** — users should be willing to talk to IT if they fear they've fallen for a social engineering attack

Tech tools and policies as another line of defense

Attackers target the human element for a reason — it requires less technical tooling and is more likely to lead to a successful attack. And because all us humans are fallible, we need another layer of protection.

Content filtering

Content filtering blocks malicious content, even if a user ends up clicking on a malicious link. You can achieve content filtering with allow/block lists, which explicitly define what websites are allowed (or not). But this has limitations. You can't possibly allow every site that's useful, nor block every possible malicious site. Plus, this isn't the internet students will see after they graduate.

What's more effective is filtering that blocks broad categories. This doesn't rely on IT admins listing specific domains. Instead, it categorizes each website and decides whether to block it based on its category. Adult websites, gambling websites, file shares, networking, violent or offensive sites, and more — they're all blocked based on your configurations. Add AI and machine learning for intelligent filtering, and you're even more golden.

Multifactor authentication

Multifactor authentication (MFA) adds an additional layer of login protection. If a user's credentials ***are*** compromised, MFA reduces the likelihood an attacker actually accesses the account. MFA requires at least two authentication methods from these:

- **Something you know**, like a password, PIN or security question
- **Something you are**, like your fingerprint or face
- **Something you have**, like another device or security key

Tech tools and policies as another line of defense

Single sign-on

Add an identity provider (IdP) to your tech stack and you can unlock true single sign-on (SSO): a single password that tells your IdP to unlock ***all*** a user's accounts. That's fewer passwords for users to remember, and therefore fewer to compromise. But doesn't that mean attackers only need one password to log into everything?

Thankfully not, since SSO generally leverages MFA. You can set it up to require a biometric like a student's fingerprint. Beyond reducing password fatigue and possible points of entry, SSO also can help prevent credential theft. Say a user ends up on a copycat site — since your IdP doesn't recognize the domain name, it won't allow the user to login and expose their credentials.

Device management

The tools we've already mentioned are great. But they're hard to implement without mobile device management (MDM). With MDM, IT admins can:

- Gain visibility into the security posture of their devices
- Set security policies and secure configurations
- Configure device settings and restrictions, like a mandated passcode or certain applications
- Keep devices up to date with the latest software
- Deploy content filtering solutions

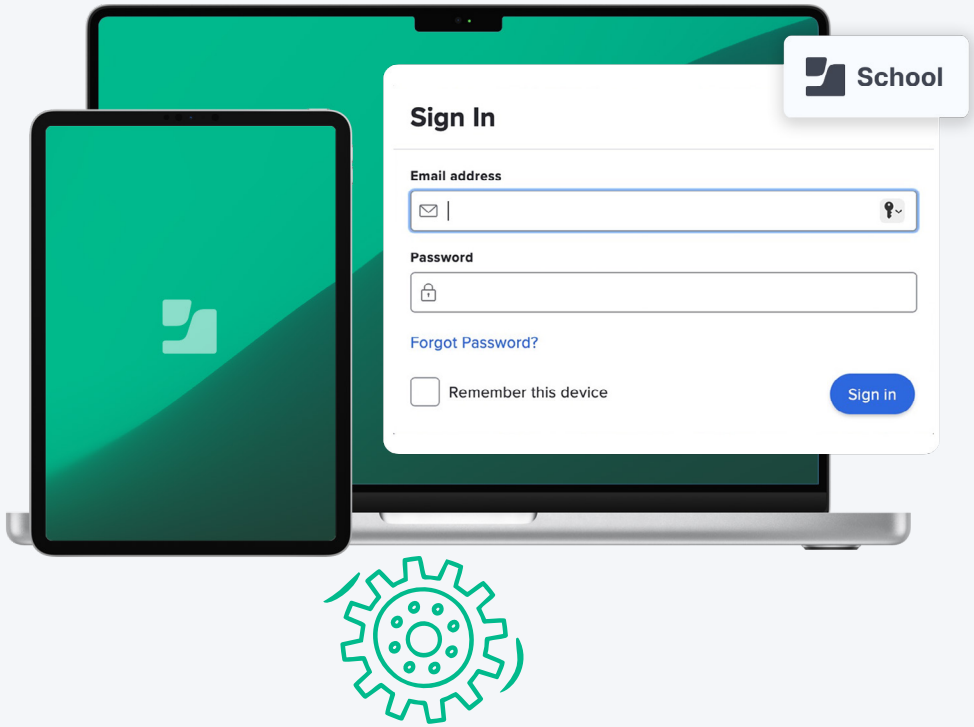
Implementation: Jamf School and Jamf Safe Internet

Jamf School

Jamf School is an MDM built for schools.
Features include:

- **Templated device configuration** that leverage declarative device management
- **Device inventory** so admins know what devices are connected to school resources
- **Transparency** into device statuses so any issues can be tended to quickly
- The ability to **set restrictions** and **settings** on a device, including a required passcode
- **Compatibility with SSO** (with additional identity provider)
- **A simple way** for teachers to request apps for IT approval
- Much **more**!

With Jamf School, your school has the foundation for secure devices that can be set up to resist social engineering attacks.

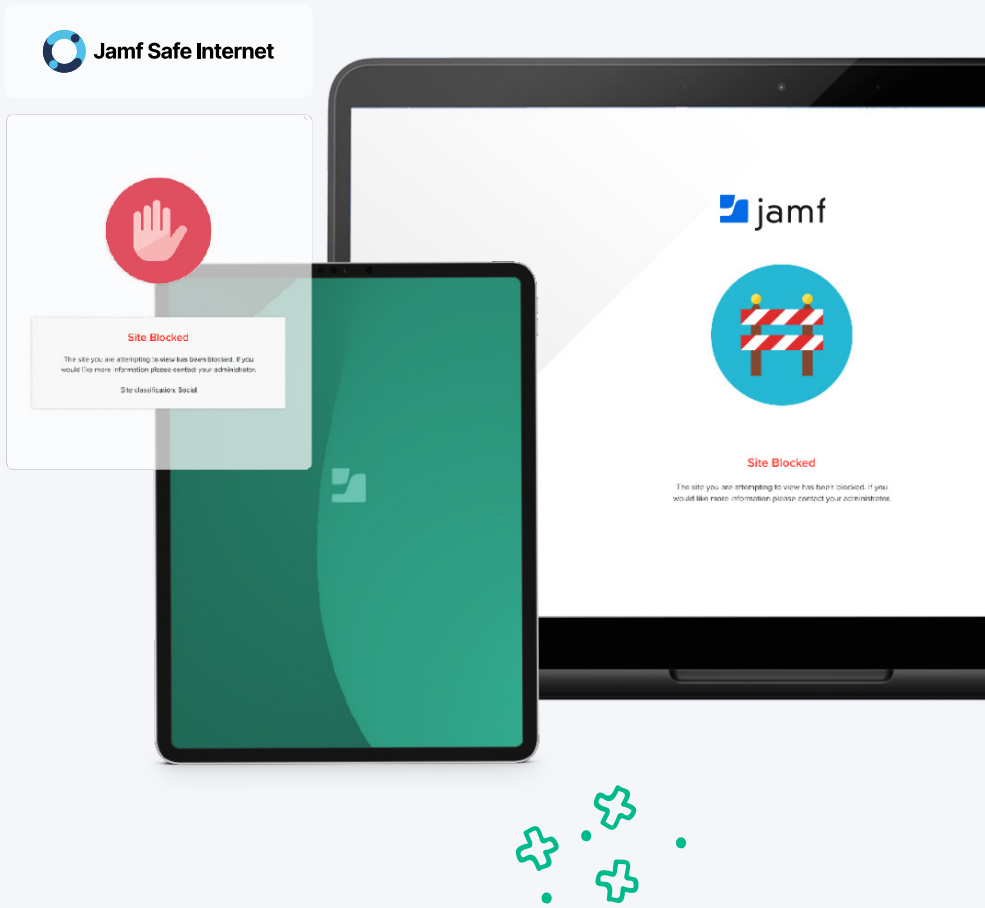


Jamf Safe Internet

Jamf Safe Internet takes security one step further, and is compatible with Apple, Chromebook and Windows devices. Jamf Safe Internet is fully customizable, making it easy to set or change policies for different device groups based on their geography, type or other attributes. It works with devices whether they live in a cart, are assigned 1:1 by the school or if they are students' own devices.

To defend against threats like social engineering, **Jamf Safe Internet offers**:

- **Powerful content filtering** backed by AI and ML — blocking access to phishing websites even before they're discovered as malicious
- **DNS** and **domain name blocking** to defend against DNS spoofing
- **On-device content filtering** on iPad for filtering anywhere
- **In-network protection** against malicious websites before they can impact devices
- Mandated **Google SafeSearch** and **Google Safe Browsing** to prevent malicious or inappropriate sites from showing up in search



All this security without surveillance: students are free to browse the internet and develop their digital citizenship skills without violating their privacy. With safe and secure technology in the classroom, everyone wins:

Teachers
can keep the focus on learning without login issues and disruptions.

Students
get the freedom to explore and learn — safely.

IT admins
can focus on other tasks, knowing their data is protected.

Want to see how technology can empower your school?

Try Jamf