Phishing in K12

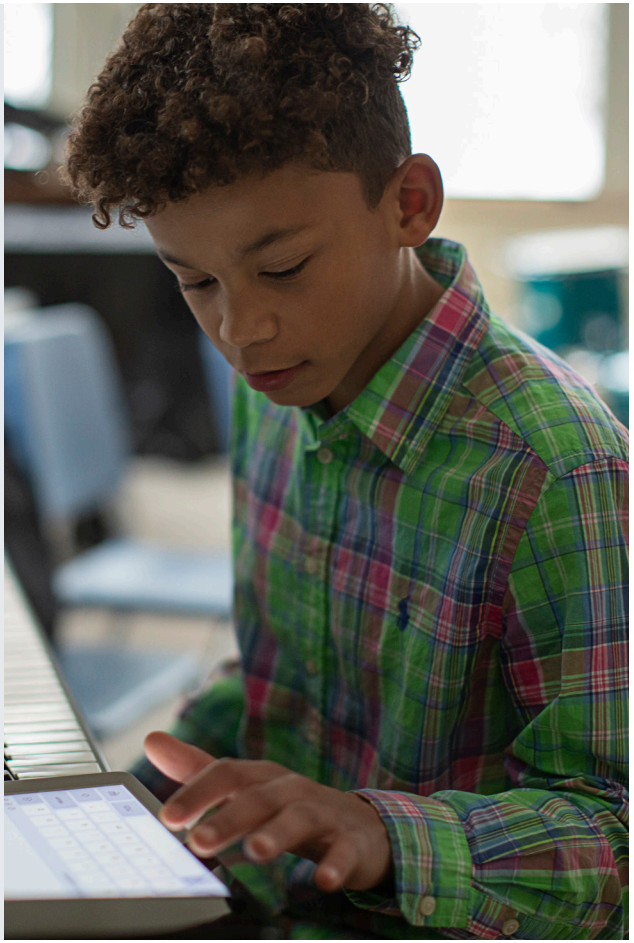
for Beginners

Greetings! This is the second e-book in our cybersecurity in K-12 schools series. In this series, we're taking a field trip through the most common cybersecurity threats schools face. **Our first stop was malware.**

As much as we'd love to grab our reels and tackle boxes, this stop is a **phishing** trip of a different kind.

jamf

IN THIS E-BOOK, WE'LL TALK ABOUT :



What is phishing?

“Phishing” is a pretty old term, at least for the lifetime of the internet. It came before the invention of Wi-Fi and the creation of websites like Google and Wikipedia. Like good old-fashioned offline fishing, phishing uses bait to lure unsuspecting parties into unfortunate consequences.

Phishing is used to gather data like banking information, login credentials, or personal identifiable information (PII) like a birthday or social security number. It’s the most common initial attack method, representing 16% of data breaches, according to the **IBM 2023 Cost of a Data Breach Report**. It’s also pricey, costing organization’s $4.76 million, on average.

Generally, phishing uses a few common tactics to make it more likely that victims take the bait:

Urgency: Attackers often demand immediate attention, threatening loss of an account, penalties for late payment, harm to a loved one or some form of negative consequence. Or, they may appeal to kindness by claiming they are in a vulnerable position and you are able to help.

Look-alikes: Website URLs may look like real URLs but have special characters. Websites or emails may be carefully crafted to look familiar, like a banking website or a password reset email.

Impersonation: Hackers might pretend to be people you know by using their email address, phone number or even voice, making it more likely you’ll respond to their phishing attempt.

Attackers use these social engineering methods for the simple reason that they often don’t require much technical knowledge. After all, it’s much easier to trick someone into giving you their account login than trying every password combination until you get it right.

Social engineering

Social engineering is a manipulation technique that uses psychological manipulation and exploits human error or weakness to gain private information, access, or valuables. It is sometimes called ‘human hacking.’

Common types of phishing attacks

Phishing attacks come in a handful of common forms. Let's go through some of them.

EMAIL PHISHING

Attackers send an email to a large group of people. This email may contain an attachment that installs malware or a link that leads them to a website made to steal their login information.

SPEAR PHISHING

Often through email, attackers target specific individuals or small groups. These emails contain content familiar to the target. For example, students and teachers might receive an email that looks like it's from software they use for school, but it contains links to a malicious look-alike website.

WHALING

These attacks focus on prominent people, like the CEO of a company. Attackers might impersonate a business partner, requesting money through a wire fund transfer. Or they may pose as a superintendent to gain information from a school principal.

WATERING HOLE

A watering hole attack is similar to spear phishing because they both develop attacks for a specific target. However, a watering hole doesn't generally start by contacting a person. Instead, attackers hack into a website where their targets gather and alters it so it steals their data or executes malware.

DNS SPOOFING

When you type a website address into your browser, your Domain Name System (DNS) software translates that address into a series of numbers that's unique to the website. DNS spoofing tricks the DNS software by changing the numbers. This means that when you type the correct address into your browser, the now compromised DNS software takes you to an attacker's site in the hope you'll enter information.

SMISHING

Smishing combines "SMS" and "phishing", meaning it's phishing that is carried out using texting. This can be tricky to spot, since links in texts are often shortened or difficult to preview.

People also use their mobile devices when they're in a hurry or on the go making it less likely they'll take the time to verify the link.

VISHING

Vishing is a combination of "voice" and "phishing," meaning phishing that uses someone's voice. This can be a stranger's voice over the phone, which can cater to people's kindness. Or, with advancements in artificial intelligence (AI), this can even be the voice of a loved one, urgently asking you to send them money.

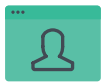
How phishing affects K-12 schools

The K12 Security Information eXchange (K12 SIX) provides cybersecurity guidance for schools. In their incident map, K12 SIX lists cybersecurity incidents K-12 schools in the United States underwent between 2016-2022. Here are some examples of how phishing affected schools:

Emails containing a phishing link were sent to teachers, allowing bad actors to **reroute teachers' direct deposits** and resulting in over $50,000 worth of stolen paychecks.

Masquerading as school administrators, attackers emailed payroll and/or HR staff **requesting employee W-2 information** — a number of schools fell victim to this request.

An attacker posing as a district contractor tricks district employees into **transferring $2.9 million to their account.** Thankfully, this is recovered.



A student uses spear phishing by creating an email account that poses as a high-ranking member of administration, requesting login information from multiple teachers. The student then uses this information to improve his grades and reduce those of other students.

A teacher complies with an email from an **attacker posing as their coworker**, asking for $500 worth of gift cards.

A common theme in these attacks is related to emails that look like they're coming from a trusted source. This could be emails attackers created with barely noticeable spelling differences or by business email compromise, where attackers gain access the actual email account.

While these attacks primarily focus on faculty and staff, student data is affected too. Phishing is a common way attackers begin ransomware attacks, resulting in data breaches that can haunt students years after the attack occurs. Attackers may use a student's information to take out loans or open credit cards, as just two examples. These students, many of them young, can't or won't know to check their credit reports for many years after the attack has occurred.

PHISHING PREVENTION

Phishing can be tricky to prevent. Schools can put up all kinds of defenses, only for someone to give an attacker their log in information.

But not all hope is lost!

Let's talk through a few ways schools can fight against the ever-present threat of phishing.

User education

Because phishing often relies on social engineering, users who can identify and stop phishing attacks are the first line of defense. After all, if users never click on phishing links, download malicious attachments or obey an attackers requests, many phishing attacks can't succeed!

Tip:
Bring phishing education to the classroom!

Here are some topics to cover:

What phishing is

Phishing is a type of scam where attackers pretend to be someone or something they aren't with the purpose of gathering private information. Attackers might pretend to be a friend, family member, coworker or person with authority. Or they might pretend to be your bank, a company you have an account with like Google, Apple or Microsoft, or another institution that might have your information. Phishing has commonly been done by email, but it can come from texts, social media, phone calls or in person. Attackers might not even contact you directly, but **may post something on social media** through one of your friend's accounts.

What to do if you suspect a phishing attempt

If you receive a suspicious email, the first thing to do is to **not click on anything** — that means no links and no attachments. If this is a school email, you should report the email to your IT department. Some schools will have a button that allows you to do this easily.

What phishing looks like

A phishing attack might be attempted by email, direct message, text, call, on a website or in person. While no two attacks are exactly identical, there are some signs to look out for:

- A message or call from someone you know at a strange time of day or night.
- A sense of urgency, such as a demand for payment or that an emergency is happening.
- Email or website addresses that look **very** similar to familiar ones, but are slightly off. These might have special characters or replace other characters: for example, it might use "0" instead of "o". Note that emails can also be totally legitimate but still be phishing if the sender's account was taken over by attackers.
- It's too good to be true — for example, all you have to do is give them some information and you'll get a $100 gift card!
- Unexpected requests, like if an email that looks like it's from a friend wants to know your address, birthdate or other personal information.

Content filtering

Unfortunately, user education can only go so far. People aren't flawless, and it takes only one successful attempt for attackers to gain access. That's where content filtering can help.

Content filtering essentially blocks access to malicious websites. For example, if a user slips up and clicks on a phishing link in an email, a content filter will recognize this and prevent access to the link.

A content filter can work in a few ways. One way is to have an allow/block list, where IT admins explicitly allow or block websites from a list. This works, but the most secure implementation means having a short allow list, which blocks off an enormous portion of the internet. This method prevents students from exploring freely — after all, once they leave school, this is the version of the internet they'll have access to.

A better method is content filtering that uses artificial intelligence (AI) and machine learning (ML). Instead of shrinking the internet to only a handful of websites, AI and ML can intelligently determine whether a site is safe to access without an IT admin having to explicitly allow or block it. Not only does this allow access to more of the web, this also blocks threatening websites that are not yet discovered. This method gives students the freedom to explore — but with guardrails. **This helps teach students how to be safe digital citizens even once they leave school.**

Single sign-on

Single sign-on (SSO) lets users log in without having to remember a password for all of their internet accounts. It can even be set up so users can log in using their fingerprint. In other words, you only have to remember your SSO password, and your SSO provider logs into the rest of your accounts for you.

This helps prevent phishing in a couple ways. SSO only works for websites and accounts it has saved. If you click on a phishing link, your SSO provider won't recognize the website and won't transfer any of your information to attackers. Since SSO can require the use of a fingerprint to log someone in, this acts as an additional factor of authentication. This makes it more difficult for attackers to successfully log into your account.

Device management

Device management is a necessary part of a school's device security. By enrolling all devices that access school resources in a Mobile Device Management (MDM) solution, IT admins gain a lot of visibility into the security standing of a device.

To have something like content filtering on a device, it needs to start by enrolling in an MDM solution. MDM software gives admins the power to configure devices, including by restricting certain settings or by adding content filtering software.

Multifactor authentication

Multifactor authentication (MFA) is a great way to reduce the chance of a successful phish. MFA requires 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

A common example is when you type your password (something you know), and receive a text containing a six-digit code on a trusted device (something you have).

Here's a scenario where MFA would help:

1. You receive an email inviting you to a shared Google document. (You don't realize it's a phishing email!)

2. You click on the link, which takes you to a site that looks like the Google login page.

3. You enter your information, but you are never taken to a document.

4. The attackers now have your information! Later, they try to log in to your account.

5. You get an MFA prompt that requires you to approve the login request.

6. Since the request is coming from a strange location or at a time you aren't trying to login, you deny the request.

The attackers are unable to access your account.

This is not a hypothetical **type of phishing scam** — it's one that has been used time and time again. In a collaborative education setting, especially, people can fall for this attack since this type of email can be common or expected.

IMPLEMENTATION: JAMF SCHOOL AND JAMF SAFE INTERNET

We've talked about a handful of ways to prevent phishing. Now let's talk implementation.

Jamf School

Speaking of device management — **Jamf School** offers MDM specially built for schools. It offers:

- 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!

The management abilities of Jamf School creates a solid foundation for secure devices, with features like SSO and device configuration reducing the impact a phishing attempt might have.

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 student's own device.

To defend against threats like phishing, 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.

jamf

See how Jamf can help be a part of your technology, security, and content filtering solution

Get Started

www.jamf.com