BANSILAL RAMNATH AGARWAL CHARITABLE TRUST'S
VISHWAKARMA INSTITUTE OF TECHNOLOGY
(AN AUTONOMOUS INSTITUTE AFFILIATED TO SAVITRIBAI PHULE UNIVERSITY)
DEPARTMENT OF INFORMATION TECHNOLOGY
FEBRUARY' 26 | IT BULLETIN

Vishwakarma Institute of Technology, Pune

Welcome to the March 2026 Edition of the IT Bulletin on

The Rise of Phishing & Digital Frauds: How Students Are the New Targets

This edition highlights the growing threat of phishing and digital frauds targeting students. With increased online activity for academics, internships, banking, and social media, cybercriminals exploit fake emails, scholarship offers, internship links, and OTP scams to steal personal and financial information.

The bulletin explains common fraud tactics and emphasizes the importance of cybersecurity awareness, strong passwords, two-factor authentication, and careful verification of suspicious links. In today's digital world, staying informed and alert is essential to protect one's data and identity.

Introduction: The Growing Threat of Digital Frauds

In today's hyper-connected digital era, technology has transformed the way we work, communicate, bank, and shop. While this digital revolution has brought convenience and speed, it has also opened doors to a rapidly increasing wave of cybercrimes. Digital frauds are no longer isolated incidents—they are a global epidemic affecting individuals, businesses, and governments alike.

In India, the rapid growth of digital transactions and smartphone penetration has significantly increased exposure to online scams. Fraudsters exploit user ignorance, weak passwords, unsecured networks, and social engineering techniques to manipulate victims into sharing sensitive information.

As digital ecosystems continue to expand, awareness and proactive cybersecurity practices are no longer optional they are essential. Organizations must strengthen their security infrastructure.

Digital fraud is not just a technical issue; it is a societal challenge that demands collective vigilance, technological innovation, and strict regulatory enforcement.

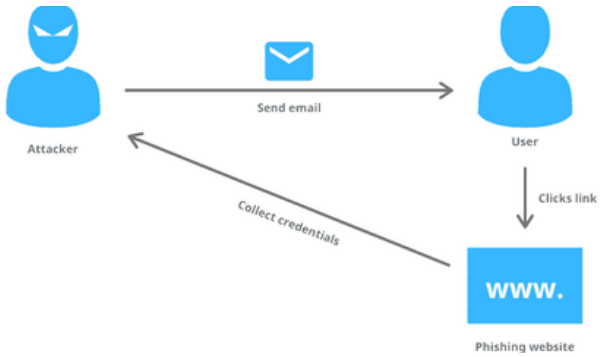
From phishing emails and fake investment schemes to identity theft and ransomware attacks, cybercriminals are becoming more sophisticated, organized, and financially motivated. With the widespread adoption of online banking, UPI payments, e-commerce platforms, and social media, personal and financial data has become a prime target.

According to global cybersecurity reports, millions of people fall victim to digital fraud each year, resulting in billions of dollars in losses. What makes digital fraud especially dangerous is its invisibility—victims often realize the damage only after financial loss or data misuse has occurred.

Understanding Phishing Attacks

Phishing is a type of cybercrime in which attackers attempt to steal sensitive information such as usernames, passwords, credit card numbers, or personal data by pretending to be a trustworthy source. These attacks usually occur through emails, messages, or fake websites that look legitimate. The goal of the attacker is to trick the victim into clicking malicious links, downloading harmful attachments, or providing confidential information.

IPhishing attacks often appear to come from banks, social media platforms, online shopping sites, or well-known organizations. The message may create a sense of urgency, such as asking users to verify their account immediately or warning that their account will be suspended. Once the victim clicks the link, they are directed to a fake website that closely resembles the real one. When the victim enters their login details, the attacker gains access to that information.



There are several types of phishing attacks. Email phishing is the most common, where fraudulent emails are sent to many users. Spear phishing targets specific individuals or organizations using personalized information. Smishing involves phishing through SMS messages, while vishing uses phone calls to trick victims into sharing sensitive details.

To protect against phishing attacks, users should always verify the sender's email address, avoid clicking on suspicious links, and check website URLs carefully. It is also important to enable two-factor authentication and keep software updated. Organizations should provide cybersecurity awareness training to help individuals recognize phishing attempts.

In today's digital world, understanding phishing attacks is essential for protecting personal and organizational information. By staying alert and practicing safe online habits, individuals can significantly reduce the risk of becoming victims of phishing scams

Why Students Are Easy Targets

Students are often considered easy targets for cyber scams because many of them spend a large amount of time online using social media, emails, and various digital platforms. They frequently download apps, join online communities, and access websites without always checking their security. Due to this high level of internet activity, scammers find more opportunities to approach students through fake messages, links, or advertisements that appear legitimate.

Another reason students are vulnerable is their limited awareness of cybersecurity threats. Many students may not fully understand how phishing emails, fake websites, or online fraud work. Scammers take advantage of this lack of knowledge by sending messages that appear to come from trusted sources such as educational institutions, scholarship programs, online shopping sites, or job offers. In some cases, students may click suspicious links or share personal information without realizing the potential risks.

Students are also more likely to be attracted to offers such as free subscriptions, gaming rewards, discounts, or part-time job opportunities. Scammers use these attractive offers to trick students into revealing personal or financial information. Because students may be eager to save money or find opportunities, they might act quickly without verifying whether the offer is genuine. Increasing cybersecurity awareness and encouraging safe online practices can help students protect themselves from becoming victims of such scams.

Common Types of Student-Focused Scams

We are warning all students to stay alert for a surge in job and housing scams currently targeting campuses. The "fake job" scam often begins with a text or email offering easy, high-paying work like a mystery shopper or personal assistant. Once you are "hired," the scammer sends a fake check and instructs you to deposit it, keep some money as pay, and send the remainder to a "vendor"—which is actually the scammer. When the check bounces days later, you are left owing the bank the full amount. Similarly, in housing scams, fraudsters post fake rental listings at attractive prices, claim they cannot show the property in person, and pressure you to wire a deposit immediately to secure the place. Never send money to someone you haven't met, and always insist on viewing a property first.

Additionally, be on high alert for urgent communications that appear to come from within the school. Scammers send emails posing as professors, deans, or the financial aid office, claiming you have an outstanding fee or a problem with your aid that requires immediate payment to avoid being dropped from classes. These emails often contain poor grammar or suspicious return addresses and may demand payment through untraceable methods like gift cards or wire transfers. Remember, legitimate institutions will never ask you to pay for anything with gift cards. If you receive a threatening or urgent message demanding money, do not click any links; instead, verify the request by contacting the department directly through official channels.

Finally, protect your personal information from phishing attempts delivered via text message. You might receive an alert claiming to be from a delivery service, Netflix, or your bank, stating there is a problem with your account or a package and urging you to click a link. These links lead to fake login pages designed to steal your username, password, and other sensitive data. Always navigate to official websites by typing the address yourself rather than clicking links in unsolicited messages. If something feels too good to be true or creates a sense of panic, trust your instincts, slow down, and report the incident to Student Services or Campus Safety.

Fake Internship and Scholarship Offers

Fake internship and scholarship offers are increasingly used by cybercriminals to target students who are searching for career opportunities and financial support. Fraudsters often send emails, messages, or advertisements on social media platforms claiming to offer attractive internships, work-from-home jobs, or guaranteed scholarships from reputed companies and universities. To appear genuine, they create professional-looking websites, use official logos, and send fake offer letters or certificates. Once a student responds, the scammers usually ask for registration fees, training charges, or verification payments. In some cases, they also request sensitive personal information such as Aadhaar numbers, bank details, resumes, or login credentials, which can later be misused for identity theft or financial fraud. Many scammers also create a sense of urgency by claiming that the offer is limited or must be accepted immediately, preventing students from verifying its authenticity. Because students are eager to gain experience and financial assistance, they often become easy targets for such scams. Therefore, students should always verify internship and scholarship offers through official websites, avoid paying upfront fees, and consult their college placement cell or trusted authorities before sharing personal information.

Fake internship and scholarship offers have become one of the most common digital frauds targeting students. Scammers create attractive messages through emails, social media, or messaging apps claiming to provide high-paying internships, guaranteed scholarships, or easy work-from-home opportunities. These offers often appear to come from well-known companies or universities and may include official-looking logos, websites, and documents to appear trustworthy. Once a student shows interest, the fraudsters usually ask for a registration fee, training fee, or personal information such as bank details, ID proofs, or login credentials. In many cases, after the payment is made, the opportunity disappears and the scammers stop responding. Since students are actively looking for internships, financial aid, and career opportunities, they are particularly vulnerable to such traps. Therefore, it is important for students to verify offers through official websites, avoid paying upfront fees, and be cautious of offers that seem too good to be true.

Social Media and Messaging App Frauds

Phishing on Social Platforms

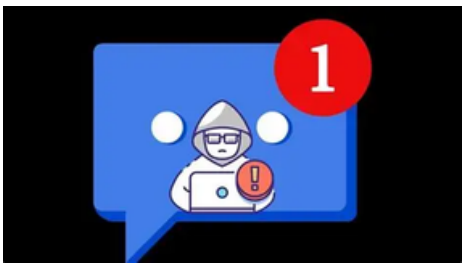
Cybercriminals create cloned login pages that mimic legitimate platforms using copied HTML and CSS. Through URL spoofing and shortened links, victims are redirected to fake domains where credentials are harvested. Once login details are captured, attackers gain unauthorized access and may reuse the same credentials across multiple platforms through credential stuffing techniques.

Social Engineering with Automation

Attackers enhance technical attacks using psychological manipulation. Fake profiles impersonate HR representatives, influencers, or trusted contacts. Automated tools help generate multiple accounts and send bulk messages. Urgency-based messages such as account suspension warnings or limited-time offers are designed to push users into revealing sensitive information without verification.

Messaging App Exploits

Messaging apps are commonly used for OTP-based account takeover attacks. An attacker initiates a password reset and convinces the victim to share the one-time password, leading to full account compromise. Malicious APK files disguised as scholarship or investment apps are also circulated; once installed, they request permissions to access SMS, contacts, and banking information, enabling financial fraud.



Student Vulnerability & Defense

Students often reuse passwords, keep public profiles, and delay enabling multi-factor authentication, increasing exposure to attacks. Protection requires strong unique passwords, two-factor authentication, verifying domains before login, avoiding unknown APK downloads, and monitoring unusual login alerts.

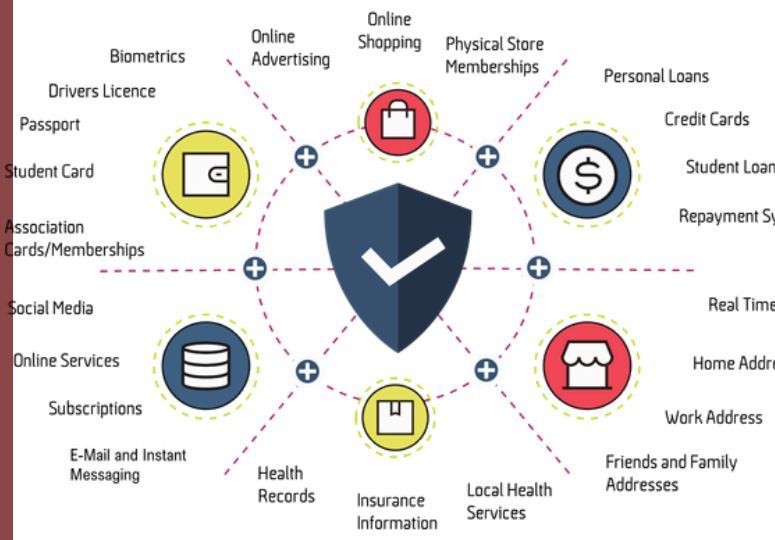
Social media and messaging frauds are automated, scalable cyberattacks that combine phishing infrastructure, malware, and data exploitation. Technical awareness and disciplined digital practices are essential for prevention.

Protecting Personal and financial information

In today's digital world, your personal and financial information is one of your most valuable assets—and identity thieves know it. Your name, address, date of birth, Social Insurance Number, and banking details can be used to open fraudulent credit accounts, make unauthorized purchases, or even file fake tax returns in your name. To protect yourself, treat this information as carefully as you would cash. Never carry your Social Insurance Number card in your wallet, and only share it when absolutely necessary for legitimate purposes like employment or banking. Be extremely cautious of anyone contacting you unexpectedly—by phone, email, or text—asking for personal details. Legitimate organizations like banks, government agencies, and utility companies will never call or email you out of the blue demanding sensitive information or immediate payment.

When it comes to safeguarding your finances, vigilance is key. Make it a habit to review your bank and credit card statements regularly, at least once a week, to spot any unauthorized transactions early. Sign up for account alerts through your financial institution so you are immediately notified of any withdrawals, purchases, or changes to your accounts. When shopping or banking online, always ensure the website is secure by looking for the padlock icon and "https://" in the address bar. Avoid conducting financial transactions over public Wi-Fi networks in places like coffee shops or airports, as these connections are often unsecured and can be easily intercepted by hackers. If you use peer-to-peer payment apps or services like e-Transfers, always double-check the recipient's information before sending money, as these payments are typically instant and irreversible.

Finally, strong digital habits are your best defense against cyber threats. Use strong, unique passwords for every online account, especially your email and banking logins. Consider using a password manager to generate and store complex passwords securely. Enable Two-Factor Authentication (2FA) or Multi-Factor Authentication (MFA) wherever possible; this adds an extra layer of security by requiring a second step—like a code sent to your phone—to access your accounts, even if your password is compromised. Be skeptical of unsolicited messages containing links or attachments, as these are common methods used to install malware or steal login credentials. By staying informed, adopting these simple practices, and trusting your instincts when something feels off, you can significantly reduce your risk and keep your personal and financial information safe.



Warning Signs of a Phishing Attempt

Phishing attempts often contain several warning signs that can help users identify them before falling victim. One common sign is receiving unexpected emails or messages that ask for personal or financial information such as passwords, bank details, or OTPs. These messages may appear to come from trusted organizations like banks, online shopping websites, or social media platforms. They often create a sense of urgency by claiming that your account will be suspended, locked, or compromised if you do not act immediately.

Another warning sign is suspicious links or attachments included in the message. Phishing emails may contain links that lead to fake websites designed to look exactly like legitimate ones. However, the website URL may contain spelling mistakes, unusual characters, or a slightly different domain name. In addition, phishing messages may have poor grammar, spelling errors, or unusual formatting, which indicates that the message is not from a professional or official source

Users should also be cautious of messages that offer deals that seem too good to be true, such as winning a lottery, receiving a prize, or getting a large amount of money unexpectedly. Attackers often use these tactics to attract attention and trick people into clicking malicious links or sharing sensitive information. By carefully checking the sender's email address, avoiding suspicious links, and verifying messages from official sources, individuals can recognize phishing attempts and protect themselves from cyber fraud.

Steps to Take If You Are Scammed

If you realize that you have been scammed, the first step is to act quickly and secure your accounts. Immediately change the passwords of any affected accounts such as email, social media, or banking applications. If financial information such as debit or credit card details has been shared, contact your bank or financial institution right away and request them to block or freeze your card or account to prevent further unauthorized transactions.

The next step is to report the scam to the appropriate authorities. In India, victims can report cyber fraud through the National Cyber Crime Reporting Portal or by calling the cybercrime helpline number 1930. Reporting the incident helps authorities investigate the fraud and may help prevent the scammer from targeting other people. Keep all evidence such as emails, messages, screenshots, or transaction details, as these can be useful during the investigation.

Finally, it is important to stay alert and carefully monitor your bank accounts, credit cards, and digital payment applications for any unusual or unauthorized transactions. If you notice anything suspicious, inform your bank or payment service provider immediately. You should also notify your contacts if the scam involved your email or social media accounts, as scammers sometimes use hacked accounts to target others. Consider enabling two-factor authentication on important accounts and updating your passwords regularly to strengthen your security. It is also helpful to learn about common online scams such as phishing emails, fake job offers, lottery scams, and fraudulent investment schemes. Being aware of these tactics can help you recognize warning signs in the future. By staying cautious, protecting your personal information, and reporting suspicious activities promptly, individuals can reduce the risk of future scams and maintain better control over their personal and financial security.

Creating a Cyber-Aware Student Community

Creating a cyber-aware student community is essential to protect young individuals from the growing threats of phishing and digital fraud. Students today spend a significant amount of time online for education, communication, and career opportunities, which makes them potential targets for cybercriminals. A cyber-aware community encourages students to understand common online threats such as phishing emails, fake internship offers, identity theft, and malicious links. Educational institutions can promote awareness by organizing cybersecurity workshops, awareness campaigns, and training sessions that teach students how to identify suspicious messages, protect their personal data, and use strong passwords. Peer discussions, student-led awareness clubs, and social media campaigns can also help spread knowledge about safe online practices. When students actively share information about new scams and support each other in identifying potential risks, it creates a safer digital environment for everyone. Building such a community not only helps prevent cybercrimes but also empowers students to become responsible and informed digital citizens.

Creating a cyber-aware student community is important in today's digital world where students frequently use the internet for learning, communication, internships, and social networking. Since students are often targeted by cybercriminals through phishing emails, fake job offers, scholarship scams, and malicious links, building awareness within the student community can greatly reduce the risk of digital fraud. Schools and colleges can encourage cybersecurity awareness by organizing workshops, seminars, and awareness campaigns that teach students how to identify suspicious emails, fake websites, and fraudulent messages. Students should also be educated about safe online practices such as using strong passwords, enabling two-factor authentication, avoiding sharing personal information on unknown platforms, and regularly updating their devices and software. Peer learning can also play a key role, where students share knowledge about new scams and help others stay alert. Creating cybersecurity clubs, online awareness groups, and campus campaigns can further promote responsible digital behavior. When students actively participate in spreading awareness and supporting each other, it helps build a safer and more informed digital environment. A cyber-aware student community not only protects individuals from online threats but also encourages responsible use of technology and prepares students to navigate the digital world safely.

REFERENCES

Federal Bureau of Investigation (FBI). (2023). Internet Crime Report. https://www.ic3.gov
– Provides statistics and information about phishing, online fraud, and cybercrime trends.

National Cyber Security Centre (NCSC). (2022). Phishing Attacks: Defending Against Deceptive Emails. https://www.ncsc.gov.uk
– Explains how phishing works and how individuals can protect themselves.

Cyber Crime Portal, Government of India. https://cybercrime.gov.in
– Official portal for reporting cybercrime and learning about common digital frauds in India.

Reserve Bank of India (RBI). (2023). Guidelines on Safe Digital Banking. https://www.rbi.org.in
– Provides awareness about online financial frauds and digital payment security.

Kaspersky. (2023). Phishing Attacks and Online Scams. https://www.kaspersky.com/resource-center
– Provides research and educational resources about phishing and cybersecurity threats.

STUDENT EDITORS

Avantika Chatterjee
SY IT-A

Kushal Chunduru
SY IT-B

Nidhish Chincholkar
SY IT-A

Aricia Dubey
SY IT-B

Pujan Sonani
SY IT-F

Arya Pawar
SY IT-A

Siddhika Tathe
SY IT-F