



Cyber Security & Awareness

**E-Newsletter**

October 2023



राष्ट्रीय डिज़ाइन संस्थान, असम  
National Institute of Design, Assam



• OCTOBER •  
**NATIONAL  
CYBER SECURITY  
AWARENESS MONTH**

“Cyber Security Awareness Month, typically observed in October, is an annual campaign dedicated to raising awareness about the importance of cybersecurity. The initiative aims to educate individuals, institutions, organizations, and communities about online threats and best practices for safeguarding their digital assets.

This year theme is: **"Secure Our World"** 

In an age where every click and keystroke hold the power to shape our lives and where data is gold and privacy is priceless, this newsletter is your armor against digital threats. Welcome to October 2023 edition of our monthly cyber security and data privacy awareness newsletter, where we bring you important updates, tips, and resources to help you stay secure in the digital world.

## Multi-factor Authentication (MFA)








Multi-factor Authentication (MFA) is an authentication method that requires the user to provide two or more verification factors to gain access to a resource such as an application, online account, or a VPN. MFA is a core component of a strong identity and access management (IAM) policy. Rather than just asking for a username and password, MFA requires one or more additional verification factors, which decreases the likelihood of a successful cyber-attack.

### Is MFA Important?

The main benefit of MFA is it will enhance your organization's security by requiring your users to identify themselves by more than a username and password. While important, usernames and passwords are vulnerable to brute force attacks and can be stolen by third parties. Enforcing the use of an MFA factor like a thumbprint or physical hardware key or OTP means increased confidence that you and your organization will stay safe from cyber criminals.



### TIPS TO CREATE STRONG AND SAFE PASSWORDS

- 1**  **CHECK FOR COMPROMISED PASSWORDS**
- 2**  **MAKE YOUR PASSWORDS LONGER**
- 3**  **MAKE YOUR PASSWORDS COMPLEX**
- 4**  **DON'T REUSE PASSWORDS**
- 5**  **CHANGE YOUR PASSWORDS REGULARLY**



**Phishing** is a type of cyber-attack where

attackers attempt to trick individuals or organizations into divulging sensitive information, such as login credentials, personal data, or financial information, by posing as a trustworthy entity. Phishing attacks can take

various forms, including email phishing, spear phishing, vishing (voice phishing), and smishing (SMS phishing). Protecting yourself and your Institute from phishing attacks is crucial.

# 10 Things to Watch

Here is a quick top ten list for how to spot and handle a phishing email.

## 1 Don't trust the display name of who the email is from.

Just because it says it's coming from a name of a person you know or trust doesn't mean that it truly is. Be sure to look at the email address to confirm the true sender.



## 6 Beware of urgency.

These emails might try to make it sound as if there is some sort of emergency (e.g., the CFO needs a \$1M wire transfer, a Nigerian prince is in trouble, or someone only needs \$100 so they can claim their million-dollar reward).



## 2 Look but don't click.

Hover or mouse over parts of the email without clicking on anything. If the alt text looks strange or doesn't match what the link description says, don't click on it—report it.



## 7 Check the email signature.

Most legitimate senders will include a full signature block at the bottom of their emails.



## 3 Check for spelling errors.

Attackers are often less concerned about spelling or being grammatically correct than a normal sender would be.



## 8 Be careful with attachments.

Attackers like to trick you with a really juicy attachment. It might have a really long name. It might be a fake icon of Microsoft Excel that isn't actually the spreadsheet you think it is.



## 4 Consider the salutation.

Is the address general or vague? Is the salutation to "valued customer" or "Dear [insert title here]"?



## 9 Don't believe everything you see.

If something seems slightly out of the norm, it's better to be safe than sorry. If you see something off, then it's best to report it to your security operations center (SOC).



## 5 Is the email asking for personal information?

Legitimate companies are unlikely to ask for personal information in an email.



## 10 When in doubt, contact your SOC.

No matter the time of day, no matter the concern, most SOCs would rather have you send something that turns out to be legit than to put the organization at risk.



## **In News Cybersecurity, Attacks, Scams**

### **FASTag scam - Man loses Rs 2.4 lakh after installing mobile app**

A man in Nallasopara lost Rs 2.4 lakh to cyber criminals while trying to recharge his FasTag account. The victim, who has not been named, was searching for the customer care number for FasTag online when he found a fake number. The 47-year-old man faced some difficulties with the recharge process. He sought assistance from 'Fastag Customer Care' via an online search. He called the number and was instructed by the person on the other end to download a remote access application on his phone. Once the application was downloaded, the cyber criminals were able to access the victim's bank account and transfer Rs 2.4 lakh to their own account and abruptly ended the call and cut off all connections.

### **New traffic e-challan fraud: Here's how to identify scam messages and avoid getting duped.**

A fake traffic police e-challan scam is being operated by cyber criminals who bank upon the people failing to notice or reading the e-challan carelessly.

The fraudulent message will read something like this – *“Your Challan No. is ... for vehicle number... having challan amount as Rs 500. For online payment of e-challan visit <https://echallanparivahan.in/> you can also contact RTO office for disposal of challan, Regards, RTO.”*

Once you click on this payment link to pay for the e-challan you will end up paying the cyber criminals instead of the police.

### **Cyber fraudsters impersonate relatives and friends, use deep fakes to scam victims.**

In the ever-evolving landscape of cyber fraud using artificial intelligence (AI) and deep fakes, fraudsters are currently impersonating relatives and friends of their victims and asking them to click on links to re-send money that was mistakenly transferred to them. Upon clicking the link, the victim's account is debited, with deep fakes helping impersonate close contacts.

### **Scammers targeting Aadhaar payment system to drain bank accounts: Here is how to lock Aadhaar online.**



Beware! Scammers are exploiting vulnerabilities in the Aadhaar-enabled Payment System (AePS) to empty bank accounts without SMS or OTP authentication. To prevent fraud, the Bengaluru Police commissioner has issued a warning, and the State Bank of India (SBI) has advised customers to lock their biometrics through the m-Aadhaar app or UIDAI portal. In these scams, criminals use victims' Aadhaar biometric data to withdraw funds without consent.

### **Cybercriminals duped a young man Rs 50 lakh by promising him handsome returns for liking and subscribing to YouTube videos.**

Cybercriminals duped a young man to the tune of Rs 50 lakh by promising him handsome returns for liking and subscribing to YouTube videos. The incident occurred in the Dhanori area of Pune. According to the police, the cyber thieves contacted Nangar on his mobile phone and offered an attractive commission for subscribing to and liking YouTube channels and videos. The complainant agreed to the job and was initially paid a commission of Rs 1,350 by the accused to gain his trust. Later the accused sent a telegram link to the complainant and him to invest almost Rs 49,68,000 on regular intervals by luring him of a high commission amount. But later refused to pay any money to the complainant.

### **Surathkal resident loses Rs 1.76 lakh in online class Scam via Telegram**

A Surathkal resident recently fell victim to an online scam, resulting in a loss of Rs 1.76 lakh when a link was shared via the Telegram app from an individual named Vyas, using the number +447541244922, on October 18. Upon attempting to reclaim the money and confronting the fraudster, the victim was informed that their account had been frozen and to reactivate it, they needed to pay an additional sum of Rs 55,000.



- If alerted promptly, bank must compensate for cyber fraud - CDRC
- Online loan fraud: Youth arrested for cheating nearly 60 people.
- Cyber police busted a fake call centre in Ujjain and arrested 7 cyber criminals.
- Coimbatore cybercrime police recover ₹33.76 lakh lost by people in online scam.



## Feeds / Images References

- <https://www.onelogin.com/learn/what-is-mfa>
- <https://safety4sea.com/infographic-ten-tips-to-detect-a-phishing-email/>
- <https://vpnoverview.com/internet-safety/secure-browsing/secure-passwords/>
- <https://cybercrime.gov.in/>
- <https://cisa.gov.in>
- <https://www.freepik.com/search?format=search&page=2&query=cyber+awareness>
- <https://sahilonline.org/surathkal-resident-loses-rs-176-lakh-in-online-class-scam-via-telegram>
- <https://www.businesstoday.in/technology/news/story/fastag-scam-man-loses-rs-24-lakh-after-installing-mobile-app-403686-2023-10-29>
- <https://www.onmanorama.com/news/kerala/2023/10/26/online-loan-fraud-thrissur-man-held-for-duping-cheating-poor-people.html>
- <https://punemirror.com/pune/crime/pune-cyber-crime-34-year-old-youth-duped-of-rs-50-lakh-by-cyber-thugs/cid1698381145.htm>
- <https://timesofindia.indiatimes.com/city/surat/if-alerted-promptly-bank-must-compensate-for-cyber-fraud-cdrc/articleshow/104711107.cms>
- <https://srilankamirror.com/news/online-courier-scam-defrauds-thousands-of-people/>
- <https://indianexpress.com/article/cities/pune/drugs-in-parcel-cyber-crime-pune-cbi-rbi-8997215/>
- <https://www.deccanchronicle.com/nation/crime/181023/hyderabad-man-loses-rs-78-lakh-in-job-offer-scam.html>
- <https://timesofindia.indiatimes.com/city/indore/7-held-for-duping-people-of-40-lakh/articleshow/104434492.cms?from=mdr>
- <https://www.thehindu.com/news/cities/Coimbatore/coimbatore-cybercrime-police-recover-3376-lakh-lost-by-people-in-online-scams/article67407578.ec>
- <https://timesofindia.indiatimes.com/city/chandigarh/woman-falls-for-pan-card-update-fraud-loses-95k/articleshow/104271586.cms?from=mdr>

In the era of technology and cyberspace, dealing with the aftermath of a cybercrime can be difficult and challenging but there is always a ray of hope for cybercrime victims to combat such attacks with various resources and initiatives in place to support and assist through law enforcement and legal action, recovery and rehabilitation, awareness, and training etc.

**Stay vigilant, stay secure.**

**Your cyber safety is our priority.**

**Keep practicing good online habits and be aware of the latest threats.**

**We'll be back next month with more tips and updates.**



Dial **1930** for Online  
financial fraud  
Report any cybercrime at  
[cybercrime.gov.in](http://cybercrime.gov.in)

**Awareness**  
is the Key to  
prevention of  
**cyber crime**

**Trust Nothing**  
**Verify Everything**

**THANK YOU**