Cyber Security Framework for UCBs-A Graded Approach

Level I Banks– Basic Controls

1. Bank Specific Email Domain

"બેંકની પોતાની ઇમેઈલ ઓળખ હોવી જરૂરી છે. Gmail અથવા Yahoo જેવી સામાન્ય ઇમેઈલ કરતાં બેંકના પોતાના ડોમેનથી ગ્રાહકોનો વિશ્વાસ વધે છે અને ફિશિંગનું જોખમ ઘટે છે." **ઉદાહરણ:** ✔ abcbank.co.in ✕ abcbank@gmail.com

ફાયદો:

ગ્રાહકોને નકલી ઈમેઈલથી બચાવી શકાય.

"બેંકનું Email Domain એ તેની ડિજિટલ ઓળખ છે. જો બેંક Gmail અથવા Yahoo નો ઉપયોગ કરે તો ગ્રાહકો માટે સાચી અને ખોટી ઇમેઈલ વચ્ચેનો તફાવત ઓળખવો મુશ્કેલ બની જાય છે."

"આજના સમયમાં Cyber Criminals બેંકની તિજોરી તોડતા નથી, તેઓ બેંકની Email System ને Target કરે છે. તેથી Bank Domain, Anti-Phishing, Anti-Malware અને DMARC એ Cyber Security ની પ્રથમ રક્ષણ રેખા છે."

"પોતાના Domain સાથે DMARC, Anti-Phishing અને Anti-Malware જેવી સુરક્ષા વ્યવસ્થા હોય તો નકલી ઇમેઈલ અને Cyber Fraud નું જોખમ ઘણું ઓછું થાય છે."

2) Anti-Phishing શું છે?

ઉદાહરણ: ગ્રાહકને ઈમેઈલ મળે: From: support@xyzbannk.co.in (અહીં xyzbank ના બદલે xyzbannk લખ્યું છે). Email માં લખ્યું છે: "તમારું KYC Update કરો નહીં તો Account Block થઈ જશે." ગ્રાહક Link પર Click કરે અને Fraud Website પર પહોંચી જાય. આને **Phishing Attack** કહે છે.

3) Anti-Phishing Solution શું કરે? નકલી Emails ઓળખે, શંકાસ્પદ Links Block કરે, અને ગ્રાહકોને ચેતવણી આપે

4) Anti-Malware શું છે?

Malware એટલે? Virus, Trojan, Spyware, Ransomware, વગેરે. **ઉદાહરણ:** એક કર્મચારી Email Attachment ખોલે:

"Salary_Revision.pdf.exe" તેમાં Virus હોય. Virus CBS Server સુધી પહોંચી શકે.

Anti-Malware શું કરે? Virus શોધે, Infection અટકાવે, Malware Delete કરે

5) DMARC શું છે?

DMARC નું સંપૂર્ણ નામ: **Domain-based Message Authentication, Reporting and Conformance** સરળ ભાષામાં: "DMARC એ બેંકના Domain નો બોડીગાર્ડ છે."

DMARC કેવી રીતે કામ કરે? ધારો કે: બેંકનું Domain: xyzbank.co.in હવે Fraudster મોકલે: ceo@xyzbank.co.in જો DMARC લાગુ હોય તો Mail Server તપાસશે: શું આ Email ખરેખર xyzbank.co.in Server પરથી આવ્યું છે? કે કોઈ Fraudster એ મોકલ્યું છે? જો નકલી હોય તો Reject અથવા Spam Folder માં મોકલી દેશે.

સરળ ઉદાહરણ, ધારો કોઈ વ્યક્તિ તમારી સહી નકલ કરીને ચેક રજૂ કરે. બેંક સહી ચેક કરે છે. સહી મેળ ન ખાય તો ચેક Reject થાય. એ જ રીતે DMARC Email ની "ડિજિટલ સહી" ચેક કરે છે.

6) RBI આ શા માટે માંગે છે?

કારણ કે ઉપર જણાવ્યા મુજબ આજે મોટાભાગના Cyber Frauds ની શરૂઆત Email થી થાય છે.

7) સામાન્ય હુમલાઓ

a) CEO Fraud -CEO Fraud એ આજના સમયમાં બેંકો અને કંપનીઓ સામેનો સૌથી ખતરનાક Email Fraud છે. **જ્યારે ઠગ CEO, Chairman, Director અથવા Senior Executive તરીકે ખોટી ઓળખ બનાવી કર્મચારીઓને પૈસા ટ્રાન્સફર કરવા અથવા ગુપ્ત માહિતી આપવા માટે છેતરે, તેને CEO Fraud કહેવામાં આવે છે."**

ઉદાહરણ – બેંકમાં ધારો કે CEO નું Email છે: **ceo@abcbank.co.in.** ઠગ નકલી Email બનાવે: ceo.abcbank@gmail.com અથવા ceo@abcbannk.co.in (એક વધારાનો "n") અને CFO અથવા Accounts Officer ને Email મોકલે: "હું હાલમાં મીટિંગમાં છું. તાત્કાલિક ₹25 લાખ Vendor ને RTGS કરો. Confidential રાખજો." કર્મચારી CEO નો Email માનીને RTGS કરી દે. પૈસા સીધા Fraudster ના ખાતામાં પહોંચી જાય. **વાસ્તવિકતા-** ઘણા CEO Fraud માં કોઈ Hacking થતું નથી. કોઈ Virus આવતો નથી. કોઈ Password ચોરાતો નથી. માત્ર **માનસિક દબાણ (Social Engineering)** નો ઉપયોગ થાય છે. ઠગ જાણે છે કે કર્મચારી CEO ની વાતને પડકારશે નહીં. આ જ કારણ છે કે RBI કહે છે: Bank Specific Email Domain, DMARC, SPF, DKIM, Employee Awareness, અત્યંત જરૂરી છે.

"CEO Fraud માં Cyber Criminal કમ્પ્યુટર નહીં પરંતુ માણસના મનને Hack કરે છે."

"ઘણા કિસ્સામાં ટેકનોલોજી નિષ્ફળ નથી જતી, પરંતુ કર્મચારીની ઉતાવળ અને વિશ્વાસના કારણે Fraud સફળ થાય છે."

b) Vendor Payment Fraud - Vendor Payment Fraud એ એવો Fraud છે જેમાં ઠગ Vendor (Supplier) અથવા Contractor તરીકે ખોટી ઓળખ બનાવી બેંક અથવા કંપનીને ખોટા ખાતામાં Payment કરાવે છે. આજકાલ આ Fraud મોટા ભાગે Email દ્વારા થાય છે અને તેને **Business Email Compromise (BEC)** Fraud પણ કહેવામાં આવે છે. **સરળ ઉદાહરણ:** ધારો કે બેંક દર મહિને CBS Vendor ને ₹5 લાખ ચુકવે છે. Vendor નું સાચું Email: accounts@abcsoftware.com છે. ઠગ Vendor નું Email Hack કરે છે અથવા તેની જેમ દેખાતું Email બનાવે છે. પછી બેંકને Email મોકલે: "અમારું Bank Account બદલાયું છે. હવે આગળની Payment નીચે દર્શાવેલ નવા Account માં જમા કરશો." Accounts Department કોઈ પુષ્ટિ કર્યા વગર Payment કરી દે. પૈસા Vendor ને નહીં પરંતુ Fraudster ના ખાતામાં જાય. **Vendor Payment Fraud માં ઠગ Vendor બનવાનો પ્રયાસ કરે છે અને Payment ની દિશા બદલી દે છે. "ખોટું Payment એકવાર થઈ જાય પછી પૈસા પાછા મેળવવા ખૂબ મુશ્કેલ બને છે." વાસ્તવિક ઘટના કેવી રીતે બને?** Fraudster, Vendor અથવા Bank ના Email પર નજર રાખે. Invoice અથવા Payment Cycle વિશે માહિતી મેળવે. ખોટું Email મોકલે- "Please note our bank account has changed." નવો

Account Number આપે. બેંક Payment કરી દે. Fraudster પૈસા ઉપાડી લે. ઉદાહરણ: સાચું Email: vendor@tcs.com નકલી Email: vendor@tcs-india.com અથવા vendor@tcs.co

I) Important Actions to be taken by a bank:

1. Call Back Verification

"Vendor નું Account બદલાય ત્યારે માત્ર Email પર વિશ્વાસ ન કરવો." Vendor ના નોંધાયેલ ફોન નંબર પર વાત કરીને પુષ્ટિ કરવી.

2. Dual Authorization: Vendor Master માં ફેરફાર માટે બે અધિકારીઓની મંજૂરી.

3. Maker-Checker Control:

4. Vendor Change Register: દરેક Account Change નો Record રાખવો.

5. Email Security: DMARC, SPF, DKIM, Anti-Phishing અમલમાં હોવા જોઈએ.

"Vendor Payment Fraud માં Invoice ખોટું નથી હોતું, Vendor ખોટો નથી હોતો, પરંતુ Payment Account ખોટું હોય છે." "જો Vendor Account Change માટે માત્ર Email મળે તો તેને ક્યારેય પૂરતો પુરાવો માનવો નહીં. 'Trust but Verify' એ Vendor Payment Fraud સામેનું સૌથી શક્તિશાળી નિયંત્રણ છે."

- Business Email Compromise (BEC) - **Email Account Compromise** ઠગ Email Hack કરે અથવા સમાન Email Address બનાવે અને પછી ફ્રોડ કરે દાખલા તરીકે CEO Fraud, Vendor Email Compromise, Fake Invoice Fraud, Payroll Fraud, etc
- Phishing- તમને લોટરી કે ઇનામ લાગ્યું છે, ઇનામ લેવા માટે નીચેની લિંક પર ક્લીક કરો, અથવા તમારું KYC અપડેટ કરવા આ લિંક પર ક્લીક કરો. તમારા પાસેથી અંગત માહિતી જેવીકે User ID, Password, OTP મેલવી લે છે. "કોઈ પણ Link પર Click કરતાં પહેલાં – મોકલનાર કોણ છે, Link ક્યાં જાય છે અને તેની જરૂર ખરેખર છે કે નહીં – તે ત્રણ પ્રશ્ન પૂછો."

UCB માટે Action Point

1. પોતાનું Email Domain હોવું જોઈએ.
2. DMARC, SPF અને DKIM અમલમાં હોવા જોઈએ.
3. Anti-Phishing Solution હોવું જોઈએ.
4. Anti-Malware Gateway હોવું જોઈએ.
5. કર્મચારીઓને શંકાસ્પદ Email ઓળખવાની તાલીમ આપવી જોઈએ.

2. Two Factor Authentication

"માત્ર પાસવર્ડ હવે પૂરતો નથી. CBS અથવા મહત્વપૂર્ણ સિસ્ટમમાં પ્રવેશ માટે OTP અથવા Token જેવી બીજી સુરક્ષા કડી હોવી જોઈએ." સ્ટાફ Login કરે: Step 1 : Password, Step 2 : Mobile OTP, બન્ને પછી જ પ્રવેશ મળે.

3. Password Management

"સાયબર સુરક્ષાની શરૂઆત મજબૂત પાસવર્ડથી થાય છે. નબળો પાસવર્ડ એ ચોર માટે ખુલ્લો દરવાજો છે."

4. Phishing Awareness

"આજકાલ મોટા ભાગના સાયબર હુમલા એક ખોટી લિંકથી શરૂ થાય છે. કર્મચારીએ કોઈપણ અજાણી લિંક પર ક્લિક કરતા પહેલાં બે વાર વિચારવું જોઈએ."

5. Cyber Incident Reporting

"સાયબર ઘટના છુપાવવી નહીં પરંતુ સમયસર જાણ કરવી એ જ સાચી સુરક્ષા છે. વહેલી જાણ નુકસાનને મર્યાદિત કરી શકે છે." UCBs shall also report all unusual cyber security incidents to CERT-In and IB-CART.

Vendor Risk Management

6. Outsourcing Responsibility

"કામ ભલે Vendor ને સોંપ્યું હોય, જવાબદારી બેંકની જ રહે છે. Outsourcing એટલે જવાબદારીનું Outsourcing નથી."

"Vendor પાસે બેંકનો ડેટા હોય ત્યારે બેંક અને RBI ને તેની તપાસ કરવાનો અધિકાર હોવો જ જોઈએ."