شریک مجرم چور ہے، ہیکر نہیں؟

بینک کارڈ ہیکنگ ایک مستقل سماجی مسئلہ ہے جس پر حکومت اور ادارہ جاتی سطح پر فوری توجہ دینے کی ضرورت ہے۔ ان واقعات کی بڑھتی ہوئی تعداد ہمارے مالیاتی اداروں کے نظام میں کمزوریوں کو اجاگر کرتی ہے اور حکومت کی طرف سے مضبوط سائبر سیکیورٹی اقدامات اور پیچیدگی کے پہلو پر توجہ اور قانون سازی کی ضرورت ہے۔

حالیہ ڈیٹا لیکس نے لاکھوں لوگوں کی حساس معلومات کو بے نقاب کر دیا ہے، جس سے ہیکرز کے لیے دھوکہ دہی کرنا آسان ہو گیا ہے۔ ایک سروے کے مطابق متحدہ عرب امارات، بحرین اور کویت ان جرائم میں ملوث افراد کے لیے ایک محفوظ پناہ گاہ بن چکے ہیں۔ کچھ معاملات میں، ہیکرز طویل عرصے سے مالیاتی اداروں میں داخل ہونے میں کامیاب ہو گئے ہیں، جس سے بڑی مقدار میں رقم چوری ہوتی ہے۔ اس سے نہ صرف اقتصادی نقصانات ہوتے ہیں بلکہ ہمارے بینکنگ سسٹمز کی سیکیورٹی پر اعتماد بھی ختم ہو جا رہا ہے۔

تحقیق سے پتہ چلتا ہے کہ قانون سازی نے دنیا بھر میں اس مجرمانہ سماجی مسئلے کے پیچھے مقامی سہولت کاروں کو نہیں بلکہ مجرموں کو نشانہ بنایا ہے۔ لہذا، یہ ضروری اور بروقت درخواست ہے کہ حکومت اور محکموں کے سربراہان اس پر غور کریں اگر وہ اس نظام کو ہموار چلانا چاہتے ہیں اور ان ممالک میں امن قائم کرنا چاہتے ہیں جو اس متعدی سماجی بیماری سے متاثر ہیں۔

اس مسئلے کو حل کرنے کے لیے، ہمیں درج ذیل اقدامات کرنے کی ضرورت ہے:

1 . **سائبر سیکیورٹی کے اقدامات کو بہتر بنائیں:** مالیاتی اداروں کو جدید سیکیورٹی پروٹوکولز میں سرمایہ کاری کرنی چاہیے اور نئے خطرات سے بچاؤ کے لیے اپنے نظام کو باقاعدگی سے اپ ڈیٹ کرنا چاہیے۔ اب وقت آ گیا ہے کہ موجودہ پروٹوکولز کا جائزہ لیا جائے اور اخلاقی اقدار کی پابندی کے ساتھ انہیں مضبوط کیا جائے۔

2 . **اخلاقی اقدار کے ساتھ جامع تحقیقات کریں:** ہر واقعے کا باریک بینی سے جائزہ لیا جانا چاہیے تاکہ یہ سمجھا جا سکے کہ خلاف ورزی کیسے ہوئی، کون سے خفیہ ہاتھ ملوث ہیں اور مستقبل کے حملوں کو روکنے کے لیے کیا اقدامات ضروری ہیں۔ مسائل کی تحقیقات کرنے والے شخص کے لیے اخلاقی اقدار پر مبنی نئے پروٹوکولز مرتب کیے جائیں۔ اخلاقی طور پر بدعنوان لوگوں کو تحقیقات کے لیے مقرر نہیں کیا جانا چاہیے کیونکہ یہ ادارے کی ساکھ، سالمیت اور اعتبار کا معاملہ ہے۔

3 . قانونی اور اخلاقی اقدار کی پابندی کے بارے میں آگاہی کو فروغ دیں**: عوام کو سائبر سیکیورٹی کی اہمیت اور اپنی ذاتی معلومات کی حفاظت کے طریقوں کے بارے میں تعلیم دینا ہیکنگ کے خطرے کو کم کرنے میں مدد کر سکتا ہے۔

4 . **اخلاقی اقدار کے ساتھ ضوابط کو مضبوط کریں:** حکومتوں اور ریگولیٹری اداروں کو سخت سائبر سیکیورٹی معیارات نافذ کرنے چاہئیں اور اخلاقی اقدار اور قانونی پروٹوکول کی خلاف ورزیوں کی عدم تعمیل پر اداروں کو جوابدہ ٹھہرانا چاہیے۔

5 . ادارہ جاتی ذمہ داری**: اداروں کو اپنی ساکھ، اعتبار اور عوام کے اعتماد کو برقرار رکھنے کے لیے مضبوط سائبر سیکیورٹی طریقہ کار نافذ کرنے، جامع تحقیقات کرنے، قانونی اور اخلاقی اقدار کے بارے میں آگاہی کو فروغ دینے اور سخت ضوابط نافذ کرنے کے ذریعے اپنے نظام کی سیکیورٹی اور سالمیت کی ضمانت دینی چاہیے۔

مندرجہ بالا سفارشات نظام کو ٹریک کرنے اور ادارہ جاتی ساکھ اور اعتبار کو برقرار رکھنے کے لیے کم از کم شرط ہیں۔ فطری طور پر، کوئی بھی دھوکہ دینا یا دھوکہ کھانا پسند نہیں کرتا، یہ وہ افراد ہیں جو ذاتی مفادات یا انتقام کے لیے اپنے اداروں کی ساکھ اور اعتبار کو خطرے میں ڈال رہے ہیں۔

سماجی ترقی امن اور خوشحالی کے ذریعے آتی ہے اور اداروں اور ریاست کے لیے ترقی کا ایک مثبت اشارہ ہے۔ لہذا، قانون ساز اور اداروں کے سربراہان اپنے اداروں کے مفادات اور ساکھ کے ذمہ دار ہیں۔

مصنف : اَرشد نعیم چوہدری، تاریخ: 1/1/2025.