انٹرنیٹ ہمارا
HAMARA INTERNET
www.hamarainternet.org

ڈیجیٹل ہراسمنٹ بھگاؤ
اور محفوظ ہو جاؤ

DRF
DigitalRightsFoundation
"KNOW YOUR RIGHTS"

MAKING ALL VOICES COUNT
A GRAND CHALLENGE FOR DEVELOPMENT

ڈیجیٹل ہراسمنٹ بھگاؤ
اور محفوظ ہو جاؤ

DigitalRightsFoundation
"KNOW YOUR RIGHTS"

معلومات برائے حق طبات و اشاعت

DigitalRightsFoundation

"KNOW YOUR RIGHTS"

کی پیشکش

بتعاون

MAKING ALL VOICES COUNT

A GRAND CHALLENGE FOR DEVELOPMENT

فہرست مضامین

ہمارا انٹرنیٹ سے متعلق

ہمارا انٹرنیٹ (Hamara Internet)، ڈیجیٹل رائٹس فاؤنڈیشن کی ایک رہنما مہم ہے جس کا مقصد خواتین کے خلاف بڑھتی ہوئی ٹیکنالوجی سے متعلق خطرات اور آن لائن تشدد کی روایات سے نبرد آزما ہونا ہے۔

ایچ آئی پی کا مقصد ایک ایسی تحریک کو تشکیل دینا ہے جو آسان اور محفوظ ڈیجیٹل ماحول کو فروغ دے جس میں خواتین آزادی کے ساتھ ڈیجیٹل دنیا میں حصہ لے سکیں۔ آگاہی مہم نشستوں، ڈیجیٹل تحفظ کی تربیتی نشستوں، تحقیق، اور ڈیجیٹل حفاظتی سامان کے ساتھ اس مہم کا مقصد خواتین کی صلاحیتوں کو سامنے لیکر آنا ہے، تاکہ ان کی آن لائن جگہ انہیں واپس دی جا سکے اور پاکستان میں بڑھتے ہوئے ڈیجیٹل دنیا میں جنسی امتیاز کو کم کیا جا سکے۔ ایچ آئی پی اس بات کو مدِ نظر رکھتی ہے کہ انٹرنیٹ ایک ایسی جگہ ہے جسے سب لوگوں کو برابری کی بنیاد پر استعمال کرنا چاہیئے۔

خراجِ تحسین

ا ر ہنما کتاب کو تشکیل دینا کبھی ممکن نہ ہوتا اگر Making All Voices Count (MAVC) کی مدد شاملِ حال نہ ہوتی۔ ان کی مکمل حمایت سے ہم اس قابل ہوئے کہ اس کتاب کو خواتین طالبات کیلئے تحریر کر سکیں جسکی بدولت ہم پر امید ہیں کہ یہ ان طالبات کی نہ صرف آن لائن بچاؤ اور تحفظ میں مدد دے گی بلکہ ان کا آن لائن مقام انہیں واپس دلانے میں بھی مدد کرے گی۔

مصنفین: نبیہہ مہر شیخ، غوثیہ راشد سلام، لعبت زاہد

ایڈیٹرز: نگہت داد، عدنان احمد چوہدری، عشبہ العین

مترجم: علی کامران

ڈیزائنر: افراء خالد

اس گائیڈ کی ضرورت

اگر چہ ڈیجیٹل سیکیورٹی پر مبنی بہت سی مفت اور آن لائن کتابیں دستیاب ہیں۔ تاہم ہمیں اس بات کا اندازہ ہے کہ پاکستانی انٹرنیٹ صارفین خصوصاً خواتین کیلئے ایک ایسی گائیڈ کا ہونا بہت ضروری تھا۔ اس ملک میں جو چیلنجز ہمیں درپیش ہیں وہ دیگر ممالک سے قطعی مختلف ہیں۔ آن لائن دیئے گئے مسائل اور ان کے حل ہمارے ثقافتی حقائق سے بالکل مختلف ہیں۔ اس کی مثال یوں دی جا سکتی ہے کہ دنیا کی کسی اور تہذیب وثقافت میں کسی بھی خاتون کیلئے فیس بک پہ اپنی تصویر ظاہر کرنے سے اسے کسی قسم کے سیکیورٹی خدشات کا سامنا نہیں کرنا پڑتا لیکن پاکستانی خواتین کیلئے (خصوصاً وہ خواتین جو اپنی تصویر فیس بک پہ نہیں رکھنا چاہتیں) یہ ایک خطرہ بن سکتا ہے۔

بہت سی خواتین نے یہ شکایت درج کرائی ہے کہ ان کے چہروں کی پروفائل تصاویر کو فوٹو شاپ کی مدد سے ان تصاویر کا غلط استعمال کیا جاتا ہے۔ ان کے چہروں کے خدوخال کو وہاں سے اٹھا کر دوسری غلط قسم کی تصاویر کے اوپر بڑی صفائی سے چسپاں کر کے بعدازاں ان خواتین کو بلیک میل کیا جاتا ہے۔ یہ جانتے ہوئے کہ ان خواتین نے کوئی غلط کام نہیں کیا لیکن پھر بھی نہ تو وہ اپنے گھر والوں سے اس معاملے پر مدد مانگ سکتی ہیں اور نہ ہی وہ قانون نافذ کرنے والے اداروں تک رسائی حاصل کر سکتی ہیں۔ کیونکہ ہماری تہذیب میں ایک خاندان کی نیک نامی ان کی خواتین کی پاکیزگی اور پاکدامنی سے جڑی ہوتی ہے اس لئے اس طرح کی بلیک میلنگ معرضِ وجود میں آسکتی ہے۔

پاکستانی خواتین کی جانب سے آنے والی شکایات نے اس گائیڈ بک کے ارتقا کی طرف ہماری توجہ مبذول کرائی۔ ہم اس بات کا اعادہ کرتے ہیں کہ مناسب قوانین کی عدم دستیابی کی وجہ سے آن لائن ہراسمنٹ کو استثنا حاصل ہے۔ مزید برآں، یہ بھی ایک حقیقت ہے کہ پاکستانی خواتین کیلئے ایسی کوئی جامع گائیڈ موجود نہیں تھی جو ان کے حل کیلئے کام کر سکتی۔ اگر چہ ڈیجیٹل سیکیورٹی کیلئے استعمال ہونے والے آلات ایک جیسے ہوتے ہیں لیکن اس میں ہمارا ثقافتی نقطہ نظر بھی شامل ہے۔ ہم نے اس میں انٹرنیٹ تہذیب کے قیام کیلئے تجاویز بھی پیش کی ہیں کہ جس سے ہمیں مزید درپیش چیلنجز کا سامنا نہ کرنا پڑے۔

تعارف

ایک معروف صحافی جہانزیب حق کا کہنا ہے کہ پاکستان میں موجود انٹرنیٹ صارفین کی کل تعداد کا ۰۷ سے ۵۸ فیصد مرد حضرات ہیں۔ پاکستانی ایف آئی اے کا کہنا ہے کہ اگست ۲۰۱۴ سے اگست ۲۰۱۵ کے دوران سائبر کرائم کے ۷۲۰۳ مقدمات درج ہوئے جن میں سے تقریباً ۵۴ فیصد صرف خواتین کو سوشل میڈیا پر پیش آنے والے سائبر ہراسمنٹ سے متعلّق تھے۔

پاکستان میں اس امر کی ضرورت ہے کہ یہاں زیادہ سے زیادہ خواتین کو آن لائن لانے، ڈیجیٹل مقامات پر زیادہ سے زیادہ حفاظتی تدابیر، اور ایسی آن لائن ثقافت کو فروغ دینا ہے جو خواتین دشمن نہ ہو۔ یہ کتاب آپ کو یہ سیکھنے میں مدد دے گی کہ خود کو آن لائن رہ کر کیسے محفوظ رکھنا ہے تا کہ پھر کبھی آپ کو اپنے آن لائن کاموں کو محدود نہ کرنا پڑے۔

ہم ایسی کئی لڑکیوں کو جانتے ہیں جنہوں نے فیس بک کا استعمال اس لئے ترک کر دیا کیونکہ ان کی پروفائل تصویر کو چرا لیا گیا تھا، یا واٹس ایپ پر غیر پسندیدہ پیغامات ملنے کے بعد انہوں نے خود پر پابندی لگا دی۔ یہ بالکل ٹھیک نہیں۔
فیس بک کے ذریعے خریداری سے لیکر واٹس ایپ پر اپنی اسائنمنٹس کے تبادلے تک جوان اور عمر رسیدہ خواتین انٹرنیٹ اور دیگر ڈیجیٹل آلات کا استعمال بہت سے کاموں کیلئے کرتی ہیں۔ بعض دفعہ جب وہ دیکھتی ہیں کہ ان جگہوں پہ آن لائن آنے سے ان کو خطرات درپیش ہوتے ہیں تو وہ سرے سے ان خدمات کا استعمال ہی ترک کر دیتی ہیں۔ ان کے حفاظتی خدشات انہیں آن لائن دنیا کے مثبت استعمال سے بھی روک دیتے ہیں۔

اس کتابچے کے ذریعے ہمارا مقصد آپ کو یہ فن سکھانا ہے کہ کس طرح آن لائن رہتے ہوئے خود کو محفوظ رکھنا ہے۔

جس طرح آپ اپنے گھر کی حفاظت کرتی ہیں بالکل ایسے ہی ڈیجیٹل لحاظ سے بھی خود کو محفوظ رکھیں۔ آپ کی مشینوں کی طرح آپ کا ڈیٹا، آپ کی سوشل میڈیا پروفائل
اور آپ کے وہ الفاظ جو آپ اپنے تبصرے کو طور پر چھوڑتے ہیں یہ سب بھی آپ ہی کا اثاثہ ہیں۔

اس سے پہلے کہ ہم بات کا آغاز کریں ایک نہایت مفید تجویز آپ کے سامنے رکھنا چاہتے ہیں: اس فن کو سیکھنے کیلئے آپ کو نہ تو ایک انجینئر بننے کی ضرورت ہے، نا کمپیوٹر سائنس میں کسی مہارت کی ضرورت ہے یا ڈیجیٹل سیکیورٹی کو مرتب کرنے کیلئے نا ہی کسی مہارت کی ضرورت ہوتی ہے۔ حتٰی کہ اگر آپ تکنیکی علم نہیں بھی رکھتیں تب بھی آن لائن سیکیورٹی اور خلوت کو یقینی بنانا ایک بنیادی امر ہے اور اس کیلئے کوئی خاص مہارت اور علم درکار نہیں ہوتا۔ لہٰذا اس بات سے نہ ڈریئے کہ ڈیجیٹل سیکیورٹی کو جاننا کوئی بہت ہی تکنیکی کام ہے، ہاں اس بات سے ضرور ڈرنا چاہئے کہ آپ کی معلومات پر کسی قسم کے سمجھوتہ کی صورت میں آپ کے ساتھ کیا کچھ ہوسکتا ہے۔

ڈیجیٹل شیڈوز

آپ کی ہر قسم کی آن لائن کارروائی اپنے پیچھے ڈیجیٹل امور سراغ چھوڑ جاتی ہے جو کہ آپ کی شناخت ظاہر کرتی ہے۔ یہ معلومات ویب سائٹس کے ذریعے جمع کی جاتی ہیں اور اجتماعی طور پر ان کو آپ کی شناخت کرنے، حتّٰی کہ آپ کے تعاقب میں استعمال کیا جا سکتا ہے۔ اسے آپ کا ڈیجیٹل شیڈو کہتے ہیں: ایسی پروفائل جو آپ کی شناخت ظاہر کرتی ہے۔ اس طرح کی معلومات ان کمپنیوں کی جانب سے لی جاتی ہیں جو آپ کی معلومات اشتہارات بنانے والوں کو بیچ کر بے پناہ منافع کماتے ہیں۔ فیس بک جیسی کمپنیاں تو باقاعدہ قانونی طور پر ایسا کرتی ہیں جبکہ غیر مقبول، چھوٹی کمپنیاں صارفین کی کم تعداد کیساتھ ایسا کرتی ہیں۔ جن پرائیویسی پالیسیوں کیساتھ ہم رضامندی کا اظہار کر کے یقین دہانی کر لیتے ہیں کہ کمپنی ہماری معلومات جیسے ہمارے کریڈٹ کارڈ کی معلومات، یا وائی فائی، یا ہمارے مقام کے بارے میں جان لے دراصل ان معلومات کو دوسری کمپنیوں کو بیچ دیا جاتا ہے۔ ادھر ہم یہ سمجھ رہے ہوتے ہیں کہ ہم ان مصنوعات کا آن لائن استعمال کر رہے ہیں لیکن دوسری طرف ہم خود مصنوعات کے طور کمپنیوں کو بیچ دیئے جاتے ہیں اور وہ کمپنیاں ہماری خریدار بن جاتی ہیں۔

اپنے ڈیجیٹل شیڈو کے متعلّق جاننا آپ کیلئے بہت ضروری ہے کیونکہ ان معلومات کو دوسرے بھی استعمال کر سکتے ہیں۔ اگر کوئی آپ کا تعاقب کر سکتا ہے تو وہ آپ کو ہراساں کرنے کیلئے بھی ان معلومات کے استعمال سے ممکنہ طور پر ایسا کر سکتا ہے۔ بعض دفعہ خواتین یہ شکایت کرتی نظر آتی ہیں کہ ان کے سابقہ شوہر کی جانب سے ان کا موجودہ مقام جاننے کیلئے ڈیجیٹل ٹریسر کا استعمال کیا گیا ہے۔
آپ اپنا ڈیجیٹل شیڈو کیسے جان سکتی ہیں؟ ڈاکسنگ تب ہوتی ہے جب کسی نقصان دہ ارادے کیساتھ کسی شخص کے متعلّق آن لائن معلومات جاری کی جائیں۔ کسی کو ڈاکسڈ کرنے کیلئے ہیک کرنے کی ضرورت نہیں پڑتی۔ آپ کے ڈیجیٹل شیڈو کا استعمال کر کے آپ کی معلومات کو آسانی سے تلاش کیا جا سکتا ہے۔

یہ جاننے کیلئے کہ آپ کی معلومات کتنی آسانی سے آن لائن دستیاب ہوتی ہیں سیلف ڈاکسنگ کر کے دیکھئے: یاد رہے، گوگل پر تلاش کرنے سے آپ کو اپنی آن لائن معلومات کی تفصیلات کے بارے میں زیادہ جانکاری نہیں ملے گی۔

DuckDuckGo جیسا سرچ انجن استعمال کریں، جو آپ کی پرائیویسی کا تحفّظ کرتا ہے۔

اپنی غیر فعال، پچھلی آن لائن پروفائلوں کی طرح اپنی فعال پروفائلوں پر اپنے تمام صارف ناموں کیلئے تلاش کریں، یہ دیکھنے کیلئے کہ کیا کچھ آن لائن ہے۔

اپنے موبائل فون اور اپنے دیگر فون نمبروں کی تلاش کریں، یہ دیکھنے کیلئے کہ آپ کے کون سے فون نمبر کی معلومات آن لائن موجود ہیں، ایک ریورس فون لُک اپ کریں۔

اپنے تمام ای میل ایڈریسز کو تلاش کریں یہ دیکھنے کیلئے کہ آپ کی ای میل کہاں بھیجی گئی ہے یا ممکنہ طور پر اس کا کہاں غلط استعمال کیا گیا ہے۔

یہ دیکھنے کیلئے کہ آپ کا پتہ یا اثاثوں کے ریکارڈ آن لائن کہاں پائے جا سکتے ہیں، اپنے گھر اور دفتر کے پتے تلاش کریں اور ایک ریورس ایڈریس لُک اپ سرانجام دیں۔

اپنے فیس بک کی کور تصاویر یا اپنی پروفائل تصاویر کی طرح اپنی مقامی تصاویر پر ایک ریورس امیج لُک اپ ترتیب دیں تا کہ یہ دیکھا جائے کہ کہیں ان تصاویر کا استعمال کہیں اور تو نہیں کیا جا رہا۔

اب آپ کو اندازہ ہو گیا ہو گا کہ آپ کا ڈیجیٹل شیڈو کیا ہے اور اسے کتنی آسانی سے دریافت کیا جا سکتا ہے، سوچئے کہ اپنے ڈیجیٹل شیڈو کے بارے میں جاننا آپ کیلئے کتنا ضروری ہے؟

یہ جاننے کیلئے کہ ڈیجیٹل شیڈو اور کتنے طریقوں سے کام کرتا ہے
Tactical Technology Collective
کا آن لائن جائزہ لیں:
https://immersion.media.mit.edu/myshadow.org

اپنی مشینوں کو محفوظ کریں

اب ہم اپنی مشینوں کی حفاظت کے بارے میں بات کرتے ہیں۔ایک چھوٹی سی غلطی آپ کی مشین کو غیر محفوظ چھوڑ سکتی ہے اور وہ ہے پاس ورڈ یا کوڈ کا استعمال نہ کرنا۔آپ کی ڈیوائس تب زیادہ غیر محفوظ ہو جاتی ہے جب آپ اسے غیر مقفّل چھوڑ جاتی ہیں۔

ایک اصول بنالیں

اپنے ہر ذاتی کمپیوٹر، لیپ ٹاپ یا موبائل وغیرہ پر ہمیشہ کوئی پاس ورڈ یا کوڈ لگا کر رکھیں۔کیونکہ اس میں آپ کا ڈیٹا پڑا ہے اور اگر کبھی وہ مشین چوری ہو جائے تو صرف مشین ہی نہیں جاتی بلکہ آپ کا قیمتی ڈیٹا بھی چلا جاتا ہے۔

سارہ کا بھائی روزانہ اس کا فون چیک کرتا تھا۔اگر کبھی وہ اپنا فون اسے دینے سے انکار کرتی تو وہ اس کے ساتھ لڑ پڑتا تھا۔وہ اس کے پیغامات اور تصاویر تک دیکھ لیتا تھا۔یہ سب کچھ جھیلنے والی سارہ کوئی اکیلی لڑکی نہیں ہے۔پاکستانی خواتین کو عموماً اپنے گھر والوں کیساتھ اپنے پاس ورڈز شیئر کرنے پڑتے ہیں۔اگر وہ ایسا نہ کریں تو ان سے زبردستی وہ معلومات لی جاتی ہیں۔

اگرچہ سارہ اس بات سے واقف ہے کہ وہ خلوت کا حق رکھتی ہے لیکن وہ اس بات سے بھی ڈرتی ہے کہ اگر وہ زیادہ مزاحمت کرے گی تو اس کے ساتھ کیا ہوگا۔وہ جانتی ہے کہ اس کا بھائی اسے سماجی کڑی نگرانی کا ہدف بنا رہا ہے اور وہ یہ بھی جانتی ہے کہ یہ سہنے والی وہ اکیلی نہیں ہے۔اس کی ایسی بھی سہیلیاں ہیں جنہیں اپنے ڈیجیٹل آلات کھلے رکھنے اور اپنے گھر کے افراد کیساتھ اپنے کوڈز وغیرہ شیئر کرنے پڑتے ہیں۔ان میں سے کئی تو اپنے خلوت کے حق کی مانگ کیلئے سرگرداں رہتی ہیں اور اس حق کی مانگ کیصورت میں آنے والے ردِعمل کا سامنا بھی کرتی ہیں۔

آرٹیکل 14

انسانی عظمت کی حرمت وغیرہ ۔۔۔۔۔۔

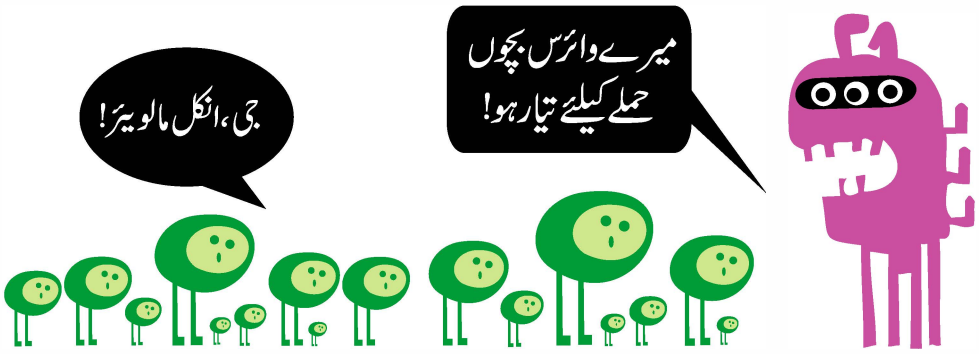
(۱) قانون کے تحت، انسانی عظمت اور گھر کی خلوت کی حرمت ہونی چاہئے۔

سارہ اپنے خلوت کے حق کے بارے میں اپنے بھائی سے بات کرنا شروع کرتی ہے۔ وہ اپنے گھر میں خلوت اور اعتماد سے متعلّق گفتگو کا آغاز کرتی ہے۔ وہ یہ جانتی ہے کہ اپنا حق حاصل کرنے کیلئے اسے کچھ وقت لگے گا اور جب کبھی وہ اپنے بھائی کو قائل نہ کر پاتی تو اسے پریشانی کا سامنا بھی کرنا پڑتا۔ پھر بھی وہ خود کو یہ باور کرواتی ہے کہ اسے اپنے حق کیلئے لڑنا ہے اور بالآخر اس کا بھائی اس پر قدغن لگانے کی بجائے اس پر اعتماد کرنے لگتا ہے۔

مستقل بنیادوں پر ایک اینٹی وائرس چلائیں:

وائرس آپ کے کمپیوٹر کو متاثر کرنے والا ایک نقصان دہ کوڈ یا پروگرام ہوتا ہے اس سے آپ کے کمپیوٹر پر ہونے والے اور ہوئے تمام کام مٹائے جاسکتے ہیں، آپ کا ڈیٹا تبدیل کیا جاسکتا ہے یا اس کا تعاقب کیا جاسکتا ہے۔ آن لائن ڈاؤن لوڈز جیسے کسی ویب سائٹ پر کوئی مفت ویڈیو یا میوزک وغیرہ کو کھولنے سے، اسی طرح ای میلز خاص طور پر سپام ای میلز کے ذریعے آپ کے کمپیوٹر پر ایک وائرس خود سے آسکتا ہے۔ اس لئے آپ ایسے کسی بھی لنک پر کلک نہ کریں جو کسی بیگانی جگہ سے آتے ہوں۔ یاد رکھیں، ایسی کسی بھی ای میل کو آگے بھیجنے سے پہلے ایک بار ضرور سوچ لیں جن میں تصاویر، ویڈیوز، آڈیو یا تہنیتی کارڈز موجود ہوں کیونکہ یہ چیزیں بعض دفعہ وائرس کے روپ میں موجود ہوتی ہیں۔

اپنے ویب براؤزر کے بچاؤ کیلئے ہمیشہ ایک اینٹی وائرس چلا کر رکھیں اور وقتاً فوقتاً اسے جدید ورژن میں اپ ڈیٹ کرتی رہیں۔ روز مرہ کے ایسے بچاؤ کے علاوہ اس بات کو ملحوظ رکھیں کہ اپنے سسٹم کو مسلسل سکین کرتی رہیں تاکہ اس بات کی یقین دہانی ہو کہ آپ کی مشین ہر قسم کے وائرس سے محفوظ ہوگئی ہے۔ ہمیشہ اچھے اینٹی وائرس سافٹ ویئر استعمال کریں جیسے:



- Kaspersky
- AVG
- Avast
- Norton Antivirus
- Avira
- Sophos

مالویئر سکین:

مالوئیر ''مالیشئس سافٹ ویئر'' کا مختصر نام ہے۔ کمپیوٹر نظام کو نقصان دینے والے مختلف قسم کے مالیشئس کوڈ یا پروگراموں کیلئے یہ ایک متّفقہ اصطلاح ہے۔ تمام وائرس مالویئر ہوتے ہیں لیکن تمام مالویئر صرف وائرس نہیں ہوتے بلکہ اس میں سپائی ویئر، رینسم ویئر وغیرہ شامل ہوتے ہیں۔

کمپیوٹروں کو اینٹی مالویئر سافٹ ویئر کی بھی ضرورت ہوتی ہے، کیونکہ زیادہ تر اینٹی وائرس روائتی خطرات جیسے Trojan وائرس، worms وغیرہ سے نبرد آزما ہوتے ہیں۔ اینٹی مالویئر سافٹ ویئر نئے خطرات پر نظر رکھتے ہیں جن میں پوری دنیا سے پیشہ ور مجرم اور ہیکرز کی جانب سے بنائے گئے بہت سی اقسام کے مالویئر شامل ہیں۔ یہ مالویئر آپ کے کمپیوٹر کو نقصان پہنچا کر اور keyloggers (keystrokes ریکارڈ کر کے آپ کا تعاقب کر سکتے ہیں یا آپ کے بنک کی معلومات چرا سکتے ہیں۔ اس لئے اینٹی وائرس کیساتھ ساتھ آپ کی مشین کی بہتر حفاظت کیلئے اینٹی مالویئر کا استعمال بھی بہت ضروری ہے۔ ہم آپ کو تجویز دیتے ہیں کہ Malwarebytes, Lavasoft اور Spybot کا استعمال کریں (اگر Malwarebytes یا Lavasoft کیساتھ اینٹی سپائے ویئر استعمال کیا جائے تو آپ کی مشین کی دوہری سکیورٹی ہو جاتی ہے)

اپنے ڈیٹا کا بیک اپ رکھنا

کیا کبھی آپ نے اپنے مضمون کو پیش کرنے سے ایک دن قبل گنوایا ہے؟ کیا کبھی آپ کا کمپیوٹر آپ کے سارے ڈیٹا سمیت خراب ہو گیا ہو؟ بعض دفعہ اپنا ڈیٹا گنوا دینا بہت تکلیف دہ ہوتا ہے اور کبھی کبھار اسے ڈیٹا کو واپس حاصل بھی کیا جا سکتا ہے۔ اسی لئے آپ کو ہمیشہ اپنے ڈیٹا کی نقول اپنے پاس محفوظ رکھنی چاہئے۔

اپنے ڈیٹا کو محفوظ رکھنے کیلئے دو طرح کے طریقے استعمال ہو سکتے ہیں

ایک تو یہ کہ تمام ڈیٹا ایک USB میں محفوظ کر لیں بعض صارف طبعی آلہ کھو دینے کے ڈر سے اس کی نسبت cloud storage کو زیادہ اہمیت دیتے ہیں، اس لئے USB جیسے آلات کو کسی محفوظ جگہ رکھنا بھی ضروری ہوتا ہے تا کہ اگر کبھی آپ کا لیپ ٹاپ وغیرہ چوری بھی ہو جائے تو آپ کا بیک اپ محفوظ رہے۔

دوسرا طریقہ یہ ہے کہ آن لائن جا کر cloud storage میں محفوظ کر لیں۔ Cloud storage اس لئے بھی سہل ہے کیونکہ اسے کسی طبعی آلے کی ضرورت نہیں پڑتی۔ اس کے ذریعے آپ کا تمام ڈیٹا آن لائن محفوظ کر لیا جاتا ہے اور Google یا Dropbox جیسی کمپنیاں آپ کے ڈیٹا کو قائم رکھتی ہیں۔

تجویز

اپنی ہارڈ ڈرائیو کو اپنے گھر کے بیڈ روم کی الماری کے کسی دراز میں محفوظ کر لیں تا کہ جب آپ کو اسے ڈھونڈنا پڑے تو زیادہ وقت نہ ہو۔

خبردار!

cloud storage دیگر حفاظتی آلے جتنا محفوظ نہیں ہے کیونکہ آن لائن ڈیٹا چرایا یا hacked کیا جا سکتا ہے۔

خبردار! ہمیشہ USB کے لین دین میں احتیاط برتیں۔ بعض دفعہ لوگ کسی کے بھی کمپیوٹر کو ہدف بنا کر نقصان پہنچانے کیلئے اس سے USB لے کر اس میں جان بوجھ کر مالویئر ڈال دیتے ہیں۔ کبھی کبھار شوہر حضرات اور منگیتر صاحبان اپنی بیویوں پر جاسوسی کی غرض سے ایسا کرتے ہیں اور کبھی کبھی سابقہ شوہروں کی جانب سے اپنی سابقہ بیویوں کو بلیک میل کرنے کیلئے ایسا کیا جاتا ہے۔ ایسے بہت سے واقعات دیکھنے میں آئے ہیں کہ جب خواتین کے کمپیوٹروں کو متاثر کر کے ان سے ڈیٹا چرا کر ان خواتین کو بلیک میل کیا گیا ہے۔ لہٰذا بہت محتاط رہیں!

ہم آپ کو شیئرڈ کمپیوٹروں پر بھی USBs کے استعمال سے آپ کو خبردار کرتے ہیں۔ ہم اس بات سے آگاہ بھی ہیں کہ یہ ایک عمومی فعل ہے اور بعض دفعہ ایسا کرنے کے علاوہ اور کوئی چارہ بھی نہیں ہوتا۔ یہاں آپ کو چند تجاویز دی جاتی ہیں:

★ مطلوبہ فائل کے علاوہ اس USB میں اور اس کمپیوٹر سے کچھ نہ ڈالیں۔

★ ہر بار استعمال سے پہلے USB کیلئے اینٹی وائرس یا اینٹی مالویئر ضرور چلائیں۔

مثال:

عتیبہ نے یہ سیکھ لیا کہ کسی USB یا بیرونی ہارڈ ڈرائیو میں اپنا ڈیٹا بیک اپ کیسے کرنا ہے لیکن وہ یہ نہ جان سکی کہ اسے اپنی فائلیں بچانے کیلئے کیا کرنا چاہئے۔

اپنی انٹرن شپ پر وہ اپنی ہارڈ ڈرائیوز اور USB اپنے نئے دفتر اپنے ساتھ لے گئی۔ یہ وہی ڈرائیوز تھیں جو کالج میں وہ اپنے کام کیلئے استعمال کرتی رہی۔ ان میں اس کے شناختی کارڈ کی نقل، اس کے مختلف تعلیمی دوروں کی تصاویر، اس کی بہت سی اسائنمنٹس اور بہت سی دیگر ذاتی معلومات پر مبنی چیزیں موجود تھیں۔

سب سے پہلا مسئلہ جو عتیبہ کو پیش آیا وہ یہ کہ دفتر کے کمپیوٹر میں لگاتے ساتھ ہی اس کی USB میں موجود تمام ڈیٹا وائرس سے بری طرح متاثر ہو گیا اور بالآخر وہ اپنے سارے ڈیٹا سے ہاتھ دھو بیٹھی۔

اس کا دوسرا مسئلہ بہت ہی واضح تھا جب اسے پتہ چلا کہ اس کے سپروائزر نے اس کے علم میں لائے بغیر اس کے شناختی کارڈ کی نقل اس کی ہارڈ ڈرائیو سے حاصل کر لی تھی۔ اگرچہ اس سپروائزر کا مقصد اسے نقصان پہنچانا نہیں تھا بلکہ محض ریکارڈ کیلئے وہ نقل حاصل کی گئی تھی۔ عتیبہ جان گئی تھی کہ کسی اور نے یہ حرکت کر کے اس کی ساری معلومات کو بڑی آسانی سے چرا لیا ہے۔

تب سے عتیبہ نے اپنی ہارڈ ڈرائیو اور USB کی حفاظت کو یقینی بنانے پر کام شروع کر دیا۔ پاکستانی خواتین کیلئے ان کا ڈیٹا اپنے مرد ہم منصبوں کی نسبت زیادہ حساس ہوتا ہے۔ مثال کے طور پر عتیبہ کے دفتری ساتھی علی کو اپنی USB کسی کو دینے اور اپنی تصاویر کو کھو دینے کا اس پر کوئی خاطر خواہ اثر نہیں ہوگا۔ لیکن عتیبہ کیلئے یہ امکان موجود تھا کہ اس کی تصاویر کو چرا کر ان کا غلط استعمال کیا جا سکتا تھا۔

پاس ورڈز محفوظ کریں

ہم میں سے بہت سے لوگ یہ سمجھتے ہیں کہ ان کے لگائے پاس ورڈز بہت مضبوط ہوتے ہیں۔ لمبے پاس ورڈز لگانا ہی کافی نہیں ہوتا؛hack کرنے والے سافٹ ویئرز پاس ورڈز میں سے ممکنہ الفاظ کے ذریعے ڈکشنری سے مدد لیکر الفاظ کو سکین کرتے ہیں اور پھر پاس ورڈز کو کریک کر کے اکاؤنٹس کو hack کر لیتے ہیں۔ایک مضبوط پاس ورڈ بنانا کوئی مشکل کام نہیں ہے خصوصاً جب آپ پاس ورڈز کی بجائے پاس فریز کا استعمال کرتی ہیں۔

ایک اصول بنالیں:

میرا پاس ورڈ ہمیشہ بہت مضبوط رہے گا اور میں کبھی بھی
اس میں کسی دوسرے کو حصہ دار نہیں بناؤں گی۔

اپنا پاس ورڈ دوسروں کے ساتھ شیئر کرنا خطرناک حد تک عام ہو چکا ہے۔ حالانکہ بہت سے لوگ یہ سمجھتے ہیں کہ اپنے قریبی دوستوں یا گھر والوں سے پاس ورڈز شیئر کرنے سے کوئی نقصان نہیں پہنچتا لیکن یاد رہے کہ کبھی اگر ان کی معلومات کو کبھی کوئی نقصان پہنچتا ہے تو آپ کی جو معلومات ان کے پاس ہوتی ہے اس کو بھی نقصان پہنچ سکتا ہے۔ دوسری بات یہ کہ ایسی عادت کو ترک کر دینا چاہئے جس سے آپ کو نقصان پہنچتا ہو۔ آپ کو اپنی پرائیویسی کا ہر صورت خیال رکھنا چاہئے اگرچہ ہمارے معاشرے میں خواتین کی پرائیویسی کو اہمیت نہیں دی جاتی۔ معاشرے میں تبدیلی تب ہی ممکن ہے جب ہم خود سے اس میں تبدیلی نہیں لائیں گی اور اپنی شخصیت میں بھی مثبت تبدیلیاں لانا ہمارے لئے بہت ضروری ہے۔

Passphrases چھ، سات الفاظ کے کرداروں پر مبنی پاس ورڈز سے نسبتاً زیادہ طویل ہوتے ہیں اور اگر انہیں صحیح ترتیب دیا جائے تو انہیں کریک کرنا قریب ناممکن ہو جاتا ہے۔ ایک مضبوط پاس فریز کچھ اس طرح سے ہوگا:

- ★ اسے ۸۱ سے ۳۰ کرداروں پر مبنی ہونا چاہئے
- ★ ایک سے زیادہ الفاظ پر مشتمل ہو
- ★ چھوٹے بڑے الفاظ، نمبر اور اشاروں پر مشتمل ہو
- ★ ایسے الفاظ پر مشتمل ہو جو ڈکشنری سے ہٹ کر ہوں یا مشہور اقوال بھی نہ ہوں

★ ذاتی، آسان اندازہ لگائے جانے والی معلومات جیسے سالگرہ، مختلف مواقعوں یا پالتو جانوروں کے ناموں پر مبنی نہ ہو

★ ذاتی ترجیحات، پسند ناپسند، مشاغل وغیرہ پر مبنی نہ ہو

★ یاد رکھنے میں آسان ہو اور کسی کاغذ پر یا اپنی ڈیوائس کے کسی مسودہ میں اس کو کبھی تحریر نہ کریں

mnemonatic device (یادداشت کا فن) بنانا پاس فریز کو محفوظ بنانے کا ایک طریقہ ہے، یہ معلومات کو یاد رکھنے کی ایک تکنیک ہے۔ مثلاً، آپ کوئی مکمّل جملہ لیتی ہیں اور پھر اس کے ہر لفظ کا پہلا، دوسرا یا آخری حرف یا نمبر کو ترتیب دے کر ایک لفظ بنا لیتی ہیں۔

مثال کے طور پر: Best friends don't ask for your password, they value your privacy and understand the importance of digital security!

اس جملے کا پاس فریز کچھ یوں بنے گا، b5D'@4up,tVURP&uti0DS

ہمیشہ یاد رکھیں

ایک سے زیادہ اکاؤنٹس کیلئے ایک جیسا ہی پاس ورڈ نہ رکھیں کیونکہ اگر ایک اکاؤنٹ ہیک ہو جاتا ہے تو دیگر اکاؤنٹس کو ہیک کرنا بھی آسان ہو جاتا ہے۔

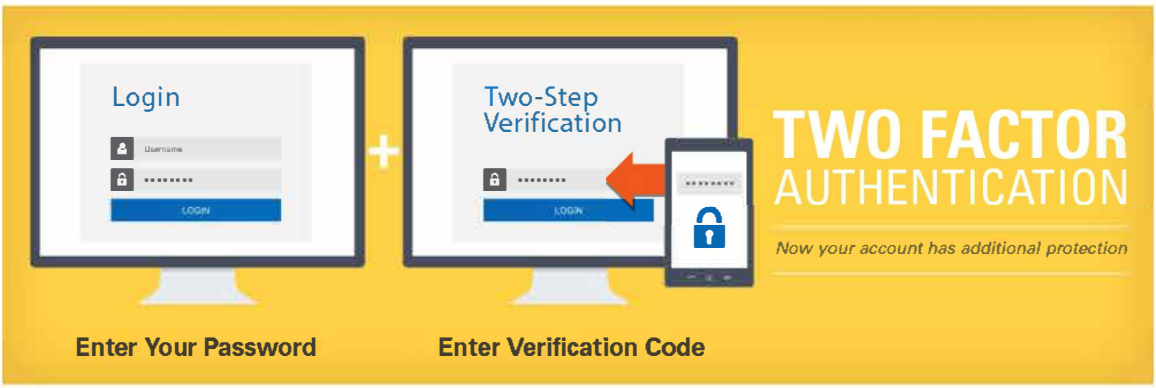
اگر زیادہ پاس ورڈز یاد رکھنا مشکل ہوں تو Keepass جیسے مفید ٹول کا استعمال کریں یہ ایک مفت پروگرام ہے جو مضبوط پاس ورڈز کو آپ کے لئے بناتا بھی ہے اور انہیں محفوظ بھی کر لیتا ہے۔ آپ کو صرف اپنا ماسٹر پاس ورڈ یاد رکھنا ہوتا ہے، یہ پاس فریز مضبوط اور ناقابلِ تسخیر ہونا چاہئے۔

اگر آپ Keepass (یا Mac کیلئے KeepassX) استعمال کرتی ہیں تو اس بات کی یقین دہانی کر لیں کہ آپ نے اپنا کی پاس ڈیٹا بیس USB یا ایکسٹرنل سٹوریج میں محفوظ کر لیا ہے۔ اگر آپ اسے اپنے کمپیوٹر میں محفوظ کرتی ہیں تو ہیکرز آپ کی سیکیورٹی کی خلاف ورزی کرتے ہوئے اس تک رسائی حاصل کر سکتا ہے۔ یاد رکھیں Keepass پاس فریز کبھی کسی جگہ پہ نہ لکھا جائے اور نہ ہی کسی کے ساتھ اس کی بابت کوئی بات کریں۔

آن لائن اکاؤنٹس محفوظ کرنا

Two-Factor Authentication:

آپ نے لوگوں کو دوطرفہ تصدیق کے بارے میں بات کرتے سنا ہوگا، یہ آپ کو شاید اس کے بارے میں پڑھنا کافی مشکل لگے گا لیکن درحقیقت اس کا طریقہ نہایت آسان ہے۔ جب آپ دوہری سیکیورٹی کیلئے اپنا موبائل فون اپنے آن لائن اکاؤنٹ کیساتھ منسلک کرتی ہیں تب وہ Two-Factor Authentication ہوجاتی ہے۔ جب آپ لاگ اِن ہوتی ہیں تو آپ کے موبائل فون پر خودکار کال یا پیغام یا کسی ایپ کے ذریعے ایک کوڈ بھیجا جاتا ہے جسے آپ کو اپنے اکاؤنٹ کو لاگ اِن کرنے کیلئے ڈالنا پڑتا ہے۔ اگر آپ اپنے ای میل یا سوشل میڈیا اکاؤنٹ پر سیکیورٹی ترتیبات میں جاتی ہیں تو آپ کو Two-Factor Authentication کو مرتب کرنے کا موقع فراہم کیا جاتا ہے۔ گوگل، فیس بک، یاہو، ٹویٹر ہاٹ میل وغیرہ آپ سے آپ کا فون نمبر پوچھتے ہیں اور پھر اسی نمبر پر آپ کو ایک کوڈ بھیجتے ہیں، یہ دیکھنے کیلئے کہ وہ صحیح بھی ہے کہ نہیں۔ ایک بار آپ اپنا موبائل نمبر دے دیتی ہیں تو سب ٹھیک ہوجاتا ہے، اگلی بار جب آپ لاگ اِن ہوتی ہیں تو پاس ورڈ ڈالنے کے بعد آپ سے ایک کوڈ پوچھا جاتا ہے۔

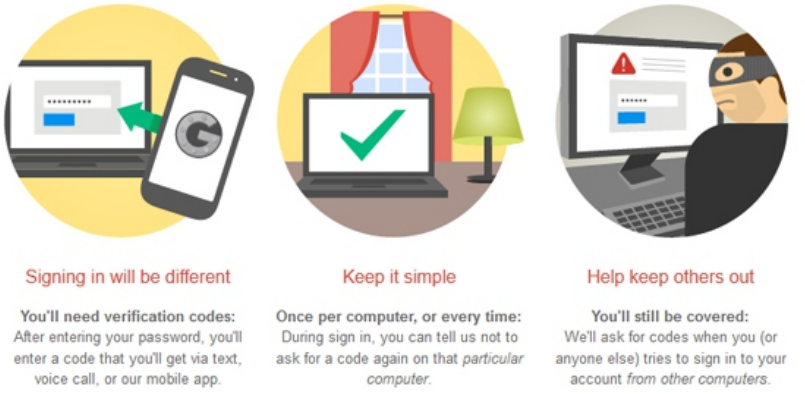


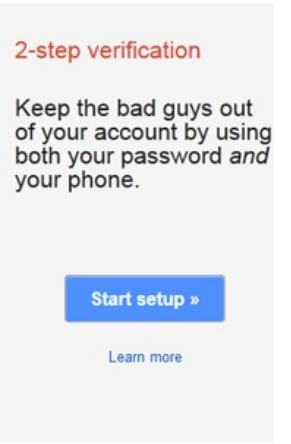
اپنے آن لائن اکاؤنٹس کو اپنے موبائل فون سے منسلک کرنا کتنا بہترین ہوتا ہے، لیکن یہ مت بھولیں کہ یہ پاکستان ہے۔ اس وقت آپ کیا کریں گی جب عید یا کسی اور تہوار کے موقع پر جب موبائل فون سگنل بلاک کر دیئے جاتے ہیں؟ یا آپ بیرونِ ملک سفر پر جارہی ہوں اور آپ دوطرفہ تصدیقی عمل کو بند کرنا بھول جائیں؟ بہت سے لوگ تو اس وقت بالکل ہی کچھ نہیں کر سکتے جب ان کے نمبر ایسے مواقعوں پر کام نہیں کر رہے ہوتے۔ ایسے ہی مواقعوں کیلئے authenticator apps بنی ہوتی ہیں۔ آپ جب بھی انہیں کھولیں گی تو یہ ایپس آپ کو ایک کوڈ دیں گی۔ جی میل Google Authenticator app استعمال کرتا ہے، جسے آپ

QR کوڈ ریڈر ایپ کیساتھ مفت ڈاؤن لوڈ کرسکتی ہیں، یہ ایپ Google Authenticator پر ہر بار آپ کو ایک نیا اکاؤنٹ مرتب کرنے کیلئے ایک کوڈ سکین کرنے میں استعمال ہوگی۔(دونوں ایپس موبائل فون کی میموری میں کافی کم جگہ گھیرتی ہیں) فیس بک اپنے اندر پہلے سے موجود کوڈ بنانے والی ایپ رکھتا ہے،لیکن یہ بھی ایک متجاوز ایپ ہے جو آپ کے موبائل کا کیمرہ اور مائک استعمال کرکے آپ کے رابطوں،کال کی تفصیلات، پیغامات،اور گیلری وغیرہ تک بغیر اجازت رسائی حاصل کرلیتی ہے۔لہٰذا وہ صارف جو فیس بک کی اس ایپ سے گریز کرنا چاہتی ہیں وہ بھی فیس بک پر کوڈ بنانے کیلئے Google Authenticator کو ترتیب دے سکتی ہیں۔

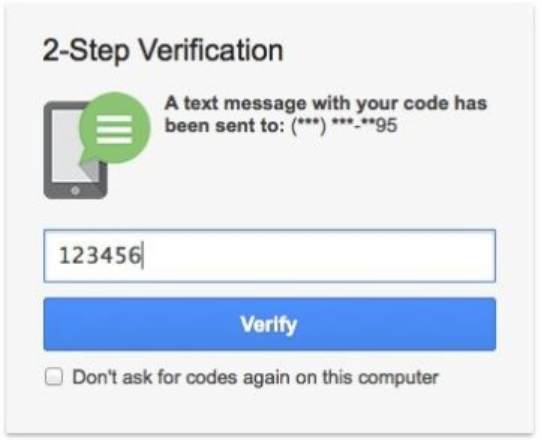
TWO STEP AUTHENTICATION FOR GOOGLE

1

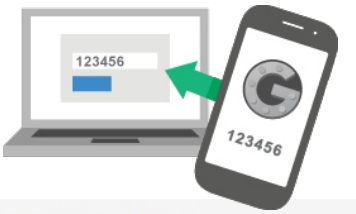


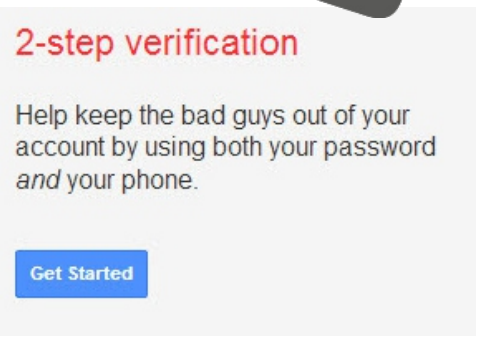


2



3





Hotmail بھی ایک تصدیقی ایپ رکھتا ہے جسے مائیکروسافٹ اکاؤنٹ کہا جاتا ہے، جو ہر بار ای میل تک رسائی کے وقت لاگ اِن درخواست کی مانگ کرتا ہے۔ٹویٹر بھی ایسے ہی کام کرتا ہے، اور آپ اپنی ترتیبات میں جائیں تو آپ ایپ میں اپنا فون نمبر ڈال سکتی ہیں اور پھر سیکیورٹی سیٹنگز سے اکاؤنٹ کی تصدیق کو قابلِ استعمال بنا سکتی ہیں۔ ہر بار جب آپ ایک براؤزر سے ٹویٹر کو لاگ اِن کرتی ہیں تو آپ کو اپنی ٹویٹر ایپ سے آئی درخواست کو ماننا پڑتا ہے۔

یاد رکھیں: Two-Factor Auhtentication کا مطلب یہ ہے کہ اب آپ کا موبائل بہت اہمیت کا حامل ہو گیا ہے۔ ہمیشہ اپنا فون لاک رکھیں، تاکہ کبھی اگر یہ گم یا چوری ہو جائے تو آپ کے ڈیٹا کو کوئی نقصان نہ پہنچے۔

ہنگامی حالات میں، جی میل اور ٹویٹر آپ کو اس بات کی اجازت دیتے ہیں کہ آپ بیک اپ کوڈز ڈاؤن لوڈ کریں جب آپ کو لاگ اِن ہونے کی ضرورت ہو۔ (یہ ان ہنگامی حالات میں استعمال ہو سکتا ہے جب مثال کے طور پر آپ کا موبائل پانی میں گر جائے اور کوئی تدبیر کارگر نہ رہے)۔ان کوڈز کو اپنے موبائل میں کبھی محفوظ نہ کریں۔ان کا پرنٹ نکال لیں یا کسی محفوظ جگہ پر لکھ لیں۔ان کو کسی خفیہ اور محفوظ مقام پر منتقل کریں۔

مثلاً: اپنا آن لائن کاروبار کرنے کے بعد رخسانہ کو غلط قسم کے پیغامات ملنے شروع ہوئے۔ بزنس کی تعلیم حاصل کرتے ہوئے اس نے سوچا تھا کہ وہ گھر سے آن لائن دوکان چلا کر بہت سے روپے کما سکتی ہے۔لیکن وہ اس بات سے نا واقف تھی کہ آن لائن کاروباری لین دین کرنا کتنے مسائل پیدا کرسکتا ہے۔

گمنامی کا لبادہ اوڑھ کر کچھ لوگ یہ سمجھتے ہیں کہ وہ آن لائن جو چاہے کر سکتے ہیں۔ایک دن رخسانہ کو غلط قسم کے اور گالیوں سے بھرے پیغامات موصول ہونے لگے اور جب رخسانہ کیلئے ان پیغامات کی بہتات نے پریشانی کھڑی کردی تو اس نے اس شخص کی پروفائل کو مکمّل طور پر بلاک کردیا۔

دوسری بات جو رخسانہ کو پتہ چلی وہ یہ کہ کسی نے اس کے فیس بک اکاؤنٹ کو ہیک کرنے کی کوشش شروع کردی ہے۔اسے ایک آن لائن نوٹیفیکیشن بھی ملا کہ کوئی اس کے جی میل پاس ورڈ کو تبدیل کرنے کی کوشش کررہا ہے۔رخسانہ جانتی تھی کہ اگر اس نے جلد از جلد کچھ نہ کیا تو نہ صرف وہ اپنے اکاؤنٹ تک رسائی کھودے گی بلکہ اپنے آن لائن کاروبار کیلئے بنائے گئے پیجز سے بھی ہاتھ دھو بیٹھے گی۔

رخسانہ کی سہیلی ماریہ نے اسے چند حفاظتی اقدامات کے بارے میں بتایا:

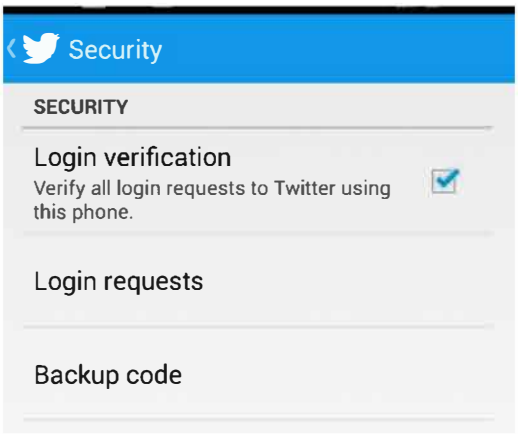
اس نے اسے بتایا کہ فوراً سے پیشتر اپنے تمام اکاؤنٹس کیلئے two factor authentication کو ایکٹیویٹ کرے۔

پھر اس نے اسے بتایا کہ جب کوئی کسی انجانے براؤزر یا کمپیوٹر سے اس کے فیس بک اکاؤنٹ تک رسائی حاصل کرلے تو اس کے لئے نوٹیفیکیشنز کو کیسے مرتب کرنا ہے۔

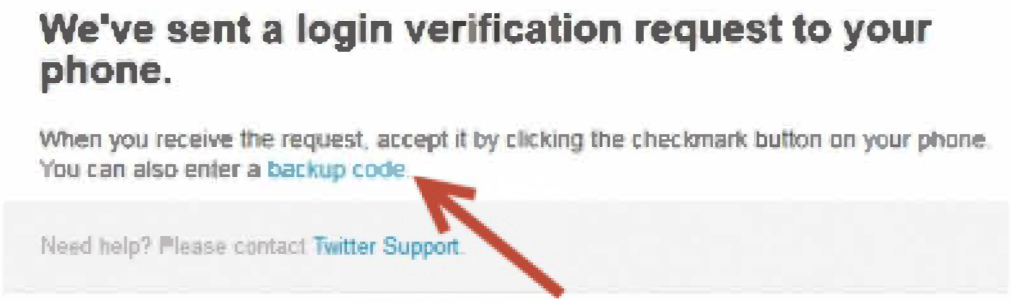
ماریہ نے رخسانہ کو یہ بھی سمجھایا کہ اسے اپنی ایپس کیلئے کوڈز کیسے بنانے چاہیئے تاکہ اسے اپنی دیگر مشینوں سے لاگ ان ہونے کیلئے ایک ہی پاس ورڈ کا استعمال نہ کرنا پڑے۔

2-FACTOR AUTHENTICATION FOR TWITTER

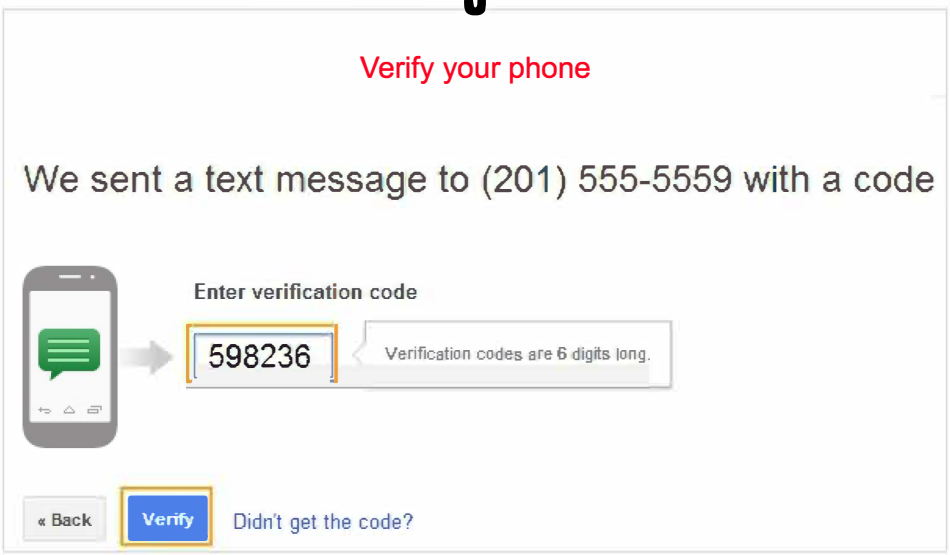
1


Security
SECURITY
Login verification
Verify all login requests to Twitter using this phone.
Login requests
Backup code

2


We've sent a login verification request to your phone.
When you receive the request, accept it by clicking the checkmark button on your phone.
You can also enter a backup code.
Need help? Please contact Twitter Support.

3


Verify your phone
We sent a text message to (201) 555-5559 with a code
Enter verification code
598236
Verification codes are 6 digits long.
« Back
Verify
Didn't get the code?

براؤزر سیکیورٹی

خواہ آپ اپنے کمپیوٹر پر وائرس اور مالویئر سے مقابلہ کرنے کیلئے ایک بہترین اینٹی وائرس چلالیں اور روزمرہ کی بنیاد پر اپنے کمپیوٹر کو سکین بھی کرلیں لیکن آپ کا براؤزر پھر بھی خطرات سے دوچار ہوسکتا ہے۔ اس لئے براؤزر کو محفوظ بنانے کیلئے اضافی اقدامات درکار ہیں۔

براؤزر سیکیورٹی کا آغاز نہایت بنیادی اقدامات سے ہوتا ہے:

1. اپنے اکاؤنٹ کو کبھی لاگ اِن چھوڑ کر نہ جائیں چاہے آپ ایک ہی ڈیوائس کیوں نہ استعمال کررہی ہوں۔ آپ اس سے کسی بھی طرح ہاتھ دھوسکتی ہیں۔ حتیٰ کہ اگر آپ نے پاس ورڈ بھی لگایا ہو پھر بھی ہر بار کمپیوٹر بند کرنے سے پہلے ہر ایک سیشن سے لاگ آؤٹ ہوجائیں یا پھر اسے سلیپ موڈ میں ڈال دیں۔

2. پرائیویٹ براؤزنگ موڈ میں جانے کیلئے (فائر فاکس میں) ایک پرائیویٹ ونڈو استعمال کریں یا (گوگل کروم میں) incognito موڈ میں جائیں۔ اس طرح آپ کا براؤزر موڈ آپ کے آنے کا کوئی ریکارڈ محفوظ نہیں رکھ پائے گا اور نہ ہی آپ کی ڈاؤن لوڈ ہسٹری محفوظ رکھ پائے گا، تاہم ابھی بھی آپ کا انٹرنیٹ خدمت مہیا کار، آپ کے کام کی جگہ یا سکول کا منتظم یا جس ویب سائٹ میں آپ گئے تھے، آپ کا تعاقب کر سکیں گے۔

3. اپنی ہسٹری کبھی محفوظ نہ رہنے دیں کیونکہ آپ کی ڈیجیٹل سیکیورٹی کو نقصان پہنچانا بک مارک کے ایک پیج کیلئے نہایت آسان ہوتا ہے۔

4. ہمیشہ اپنی عارضی انٹرنیٹ فائلیں اور کوکیز کو ختم کردیں۔

5 اگر آپ چاہتی ہیں کہ ویب سائٹس کے ذریعے آپ کا تعاقب نہ ہو تو براؤزر ترتیبات میں جا کر "do not track" آپشن کو enable کر دیں۔

6 اس بات کی یقین دہانی کر لیں کہ آپ نے ممکنہ حملہ آور ویب سائٹس اور ویب جعلسازی کو بلاک کرنے کیلئے تمام آپشنز کو آن کر دیا ہے۔

7 کسی ایسی ویب سائٹ پر اپنا پاس ورڈ کبھی داخل نہ کریں جس کی آفیشل ای میل یا آفیشل سوشل میڈیا ویب سائٹ نہ ہو۔ کیونکہ یہ راستہ آپ کی کسی بھی حساس معلومات خصوصاً کریڈٹ کارڈ معلومات تک جاتا ہے۔

BROWSER ADD-ONS

براؤزر سیکیورٹی میں اگلا قدم add-ons یا extensions ہوتا ہے۔ آپ شاید ویڈیوز یا میوزک ڈاؤن لوڈ کرنے کیلئے براؤزر add-ons پہلے سے ہی استعمال کرتی ہوں۔ اسی طرح کوکیز، ٹریکرز اور پاپ اپ اشتہارات بلاک کرکے اپنی پرائیویسی اور دفاع کو بچانے کیلئے براؤزر add-ons ہوتے ہیں۔ یہاں چند add-ons دیئے جارہے ہیں جو آپ کے براؤزر کو ضرور رکھنے چاہئیں۔

HTTPS EVERYWHERE:

یہ یقین دہانی کراتا ہے کہ آپ HTTPS کے ذریعے انک وب سائٹ سے محفوظ طریقے سے منسلک ہوگئی ہیں، ایسا کرنے سے جہاں تک ممکن ہوسکتا ہے آپکی معلومات HTTP جیسی غیر محفوظ کی نسبت زیادہ نجی اور محفوظ رکھی جائے گی۔

PRIVACY BADGER:

یہ add-on یقین دہانی کراتی ہے کہ دوسری ویب سائٹس آپ کا تعاقب نہیں کریں گی۔

جب آپ فیس بک کے Share بٹن پر کلک کرتی ہیں، یا سیدھے ہی کسی ویب سائٹ سے کوئی ٹویٹ کرتی ہیں تو آپ کا ردِعمل ریکارڈ کرلیا جاتا ہے اور آپ کی آن لائن حرکات دیکھنے میں استعمال ہوتا ہے تاکہ آپ کا ایک ڈیجیٹل شیڈو بن جائے۔ یہ کتنی ناگوار بات ہے! PB اور GHOSTERY جیسی Add-Ons اس بات کو یقینی بنائیں گی کہ کوئی ویب سائٹ آپ کا تعاقب نہیں کرپائے گی۔

کیا آپ جانتی ہیں!

NO SCRIPT:

سکرپٹ ایک ایسا چھوٹا پروگرام ہے جنہیں چند ویب سائٹس آپ کے براؤزر پر چلادیں گی۔ بعض دفعہ یہ سکرپٹس دفاعی کمزوریاں رکھ سکتی ہیں، اور یہی وجہ ہے کہ آپ کو نوسکرپٹ کی ضرورت پڑتی ہے، تاکہ نوسکرپٹ بغیر کسی اجازت کے آپ کے براؤزر میں چل سکے۔

سوشل میڈیا سیکیورٹی اور گمنامی

اگر آپ اپنے دفاع کے بارے میں بہت زیادہ مطمئن ہیں تو یہ جان لیں کہ سوشل میڈیا نہ صرف ایک مذاق بلکہ کافی مسائل پیدا کر سکتا ہے۔ یہ بھی ایک بہت اہم بات ہے کہ سوشل میڈیا اپنی دفاعی اور پرائیویسی ترتیبات میں وقتاً فوقتاً تبدیلیاں لے کر آتے ہیں یعنی جو چیزیں پہلے بہت زیادہ یا صرف خاص لوگوں کو دکھانے کیلئے ہوتی تھیں ان پلیٹ فارمز کی لمحہ بہ لمحہ بدلتی حکمتِ عملیوں کے باعث وہی معلومات عوامی بھی بن سکتی ہیں اور انہیں کوئی بھی دیکھ سکتا ہے۔ مندرجہ ذیل آن لائن دفاع کیلئے چند تجاویز دی جا رہی ہیں:

★ اگر آپ عوامی پوسٹ کا استعمال زیادہ پسند کرتے ہیں تو اس بات کو مدِ نظر رکھیں کہ ان پوسٹ میں آپ کس قسم کی معلومات ڈال رہے ہیں۔ عوامی پوسٹ میں اپنی ذاتی یا قابلِ شناخت معلومات نہ ڈالئے کیونکہ اس تک عام عوام کی رسائی بھی ہو سکتی ہے۔ ان معلومات میں آپ اور آپ کے دوستوں کی تصاویر کی طرح عوامی تصاویر بھی شامل ہوتی ہیں۔

★ اپنی دفاعی اور پرائیویسی ترتیبات کو روزانہ کی بنیاد پر دیکھتے رہیئے تا کہ وہ اپ ڈیٹ رہیں اور اس بات کی یقین دہانی بھی ہو جائے کہ ویب سائٹس کی تبدیلیوں کا آپ پر کوئی فرق نہیں پڑا۔

★ گمنامی رکھ کر آپ صارفین سے اپنے ای میل ایڈریس یا فون نمبر یہاں تک کہ اپنی دفاعی ترتیبات کے ذریعے انہیں پیغامات بھیجنے سے روک سکتی ہیں اور اس طرح اپنا دفاع کر سکتی ہیں۔

★ فیس بک آپ کو یہ دیکھنے کی اجازت دیتا ہے کہ آپ کہاں سے لاگ اِن ہوئی ہیں اور کس براؤزر پر آپ لاگ اِن ہوئے ہیں۔ اس بات کو مستقل بنیادوں پر ذہن میں رکھئے کہ آپ نے کبھی حادثاتی طور پر بھی کسی سیشن کو کسی بھی جگہ پر لاگ اِن نہیں چھوڑا ہوگا یا آپ کے اکاؤنٹ کو کبھی کوئی نقصان نہ ہوا ہوگا۔

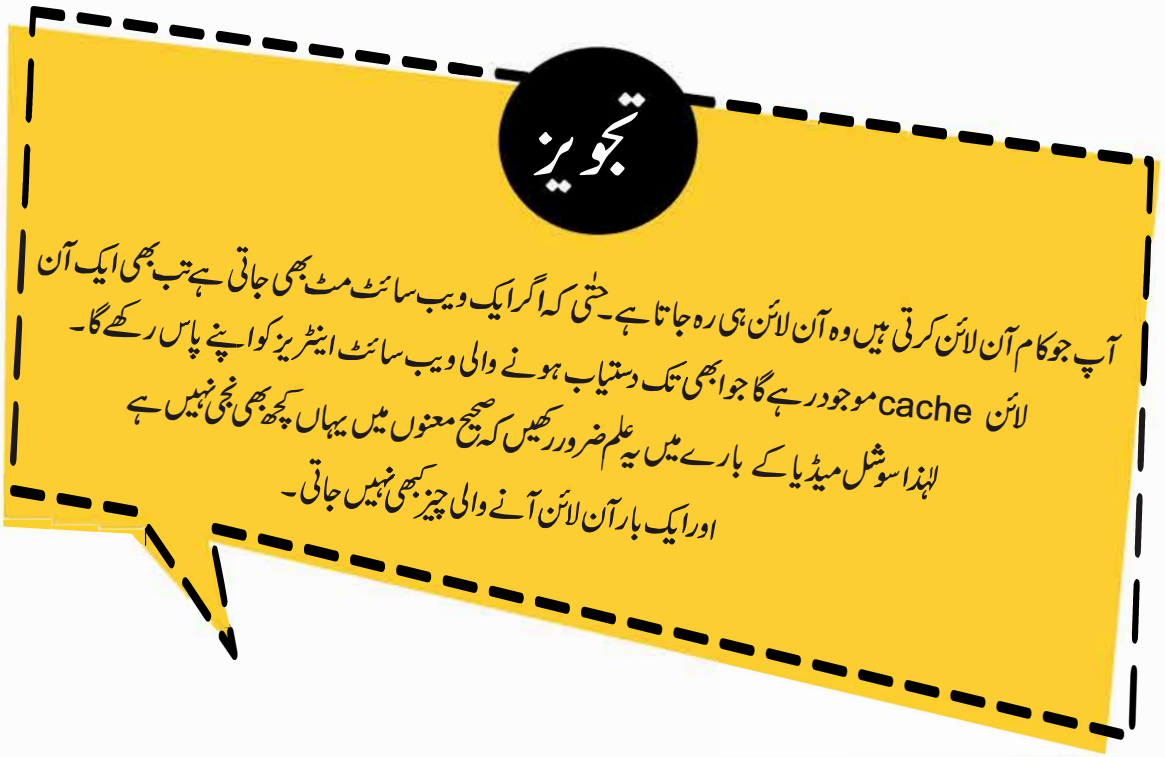
★ اس بات کی یقین دہانی کر لیں کہ سوشل میڈیا ویب سائٹس آپ کا آن لائن تعاقب یا ذاتی اشتہار نہیں بنا سکتیں۔ اپنی فیس بک preferences چیک کریں آپ یہ دیکھ کر ڈر جائیں گی کہ آپ کی "ad preferences" شناخت کرنے کیلئے ایک بڑی تعداد میں keywords کا استعمال کیا جاتا ہے۔

★ سوشل میڈیا ویب سائٹس کو اپنے مقام کا تعاقب نہ کرنے دیں اور اس بات کو یقینی بنائیں کہ ایسے تمام آپشن ڈس ایبل ہو گئے ہیں۔

★ اس بات کا اعلان کبھی نہ کریں کہ آپ سوشل میڈیا میں کہاں پر موجود ہیں، خصوصاً جب آپ کسی ایونٹ کی براہِ راست اپ ڈیٹنگ نہ کر رہی ہوں۔ یہاں تک کہ گھر واپسی پر بھی جب آپ اپ ڈیٹ ڈال رہی ہوں تب بھی اس بات کا اعلان نہ کریں ورنہ

آپ کونقصان پہنچانے والے ہیکرز یا سٹاکرز آپ کی حالیہ نشست کو دیکھتے ہوئے آپ ہی کی ایک پروفائل بنا سکتے ہیں۔ یہ آپ کیلئے آف لائن خطرات کے حامل بن سکتے ہیں۔

★اپنی ٹیگ ترتیبات کا معائنہ کرلیں تا کہ اس بات کی یقین دہانی ہو سکے کہ آپ نے غیر ضروری تصاویر یا اپ ڈیٹس ٹیگ اِن نہیں کیں۔



VPNS:

دوسرے ممالک میں سرورز سے اپنے براؤزرز کو ہدایت دلوانے اور اپنے مقام کی دستیابی کو چھپانے کیلئے آپ VPN (Virtual Private Network) کا استعمال کرسکتے ہیں۔آپ Hot Spot Shield جیسا ایک VPN اپنے کمپیوٹر میں شامل کرسکتی ہیں لیکن ہوشیار رہیں کہ یہ آپ کے کمپیوٹر کی رفتار دھیمی کرسکتا ہے۔اس کے علاوہ اپنے براؤزر میں zenmate جیسا ایک VPN شامل کرنے کا بھی اختیار آپ رکھتی ہیں۔

ہماری یہ تجویز ہے کہ اپنی ڈیوائس کو اپنے مقام تک رسائی حاصل نہ کرنے دینا ایک اچھی مشق ہے۔ حالانکہ آپ کے فون یا دیگر ڈیوائسز پر آپ کو آن لائن نقشوں سے ہدایات حاصل کرنے کیلئے اپنے مقام کے بارے میں بتانے کی ضرورت ہوتی ہے، لیکن ہم یہ بھول جاتے ہیں جب ہم آف لائن ہو جاتے ہیں تب بھی ہم ان ایپلیکیشنز کو اپنے مقام تک رسائی کی اجازت دے رہے ہوتے ہیں۔ اس طرح اگر ہم اپنی لوکیشن خدمات کو بند نہیں کرتے تو ہماری ڈیوائسز کا تعاقب کر کے ہمارے طبعی مقام کا با آسانی پتہ چلایا جا سکتا ہے۔

سائبر ہراسمنٹ اور محفوظ مقامات

آپ تصور کریں کہ جب کوئی چاہے آپ کے دروازے پر دستک دے اور آپ کے دروازہ کھولنے پر وہ آپ پر برس پڑے، آپ کو گالیاں دے اور آپ کی بے عزتی کرے۔ یا فرض کریں کوئی آپ کے گھر کے باہر کھڑا ہو کر دن رات آپ پر گالیوں کی بوچھاڑ کرتا ہو۔ لامحالہ ایسی صورتِ حال میں آپ پولیس کو اطلاع کریں گی اور دیگر لوگ آپ کی مدد کریں گے یا اس شخص کو جانے کیلئے کہیں گے۔ اس میں کوئی شک نہیں کہ ہم اپنے ظاہری مقام پر پیدا ہونے والے خطرات اور پریشانیوں کو بہت سنجیدگی سے لیتی ہیں لیکن جب بات سائبر سپیس کی ہوتی ہے تو اسے سنجیدگی سے نہیں لیتیں۔ ہم اس بات سے بھی بخوبی آگاہ ہیں کہ ہر کسی کا اپنا طبعی مقام ہوتا ہے اور ہم یہ بھی جانتی ہیں کہ ہمیں کسی کے طبعی مقامات یعنی گھروں اور دفاتر میں نہیں گھسنا چاہئے۔ اسی طرح ہم کسی کے گھر بن بلائے نہیں جاتے اور ہم میں سے بہت سے لوگ دوسروں کو رات گئے تک فون بھی نہیں کرتے کیونکہ ہم ان کے مقام اور خلوت کا احترام کرتے ہیں۔

اس کے علاوہ جب کوئی سائبر بُلیڈ یا ہراساں ہونے کی بات کرتا ہے تو اسے اکثر مؤردِ الزام ٹھرایا جاتا ہے کیونکہ وہاں کسی طبعی مقام کو نقصان نہیں پہنچتا۔ سوشل میڈیا اور عام انٹرنیٹ لہجہ مرتب کرنے کیلئے لامحالہ صارفین پر انحصار کرتے ہیں۔ یہ ہماری بدقسمتی ہے کہ جو لہجہ انٹرنیٹ پر ترتیب دیا جاتا ہے وہ خصوصاً خواتین کیلئے کوئی خوش آئند نہیں۔

اگرچہ یہاں کوئی اس لئے نہیں آتا کہ اسے گالیوں یا دھکوں سے نوازا جائے لیکن پھر بھی ہمیں اکثر دلکش بیہودہ گالیوں کا نشانہ بنایا جاتا ہے۔ کیا اپنے خیالات کے اظہار پر آپ پر کبھی کوئی حملہ کیا گیا ہے؟ ہم جانتے ہیں کہ آپ کو اس وقت کتنا برا لگا ہوگا۔ بعض دفعہ تو ہمیں ان گالیوں سے مزید بچنے کیلئے ایسے لوگوں کو بلاک کرنا پڑتا ہے۔

بعض مافوق الفطرت تو اتنے بے رحم ہوتے ہیں کہ بلاک کئے جانے کے باوجود نئی پروفائل بنا لیتے ہیں۔ آپ ذرا سوچئے وہ ایسا کیوں کرتے ہیں۔ وہ کیوں بار بار گالیاں دیتے ہیں؟ کیا اس لئے کہ وہ غم و غصے سے بھرے ہوتے ہیں؟ یا شاید وہ آپ کو وہاں سے چلتا کرنا چاہتے ہیں؟ ہم سمجھتے ہیں کہ وہ آپ کو خاموش کرانا چاہتے ہیں تو خاموش رہ کر مزاحمت کرنے میں کوئی مضائقہ بھی نہیں۔

جب لوگ کسی غیر مقبول رائے کا اظہار کرتے ہیں تو صارفین اکثر ایسے لوگوں کو چپ کرانے کیلئے بلوائیوں کا سہارا لیتے ہیں۔ لوگ آن لائن دھمکیاں دیتے ہیں کہ دوسرا بندہ زبانی کلامی بھی اپنی رائے نہ دے، بعض دفعہ تو ایسی بھی دھمکیاں دیکھنے کو ملتی ہیں کہ ایسا کرنے سے وہ اپنی موت کو دعوت دے رہے ہیں۔

یاد رکھیں:

اگر کوئی آپ کو آن لائن تنگ کرے یا کوئی ایسی بات کرے جس سے آپ کو پریشانی کا سامنا ہو تو یہ آپ کا قصور نہیں ہے، آپ خواہ ایسی رائے کا اظہار کر رہے ہوں جو دوسروں کو ناپسند ہو تب بھی آپ ایسے سلوک کے مستحق نہیں۔

ذرا سوچئے: آپ پر گالیوں کی بوچھاڑ کی جا رہی ہو محض اس لئے کہ آپ کے الفاظ یا آپ کی رائے جو صرف آپ کی ملکیت ہیں ان کو ہدف بنایا جا رہا ہو۔ آپ کو صرف اس لئے نشانہ بنایا جا رہا ہوتا ہے کیونکہ زیادہ تر صارفین جانتے ہیں کہ یہاں ان کی بات زیادہ سنی جائے گی اور ان کی حوصلہ افزائی بھی ہوگی۔ وہ یہ بھی جانتے ہیں کہ آپ کے طبعی مقام پر آپ پر حملہ کرنے سے ان کیلئے مسائل کھڑے ہوں گے۔ مثلاً، اگر وہ آپ پر لیکچر ہال میں برسیں گے یا برا بھلا کہیں گے تو ان کی باز پرس ہوگی۔ لوگ بولیں گے اور آپ کو حمایت بھی ملے گی۔

بُلیز جیسے مافوق الفطرت لوگ دوسروں پر اپنی طاقت کا مظاہرہ کر کے خوش ہوتے ہیں۔ وہ دوسروں کو پریشان کر کے انہیں خوشی ملتی ہے۔ یہ بھی بُلنگ کرنے کے مترادف ہے کیونکہ ہم اس بات سے آشنا ہیں کہ بُلنگ کرنے سے گالیوں کے ایک دورانئے کی تخلیق ہوتی ہے۔ کوئی بھی شخص ایسی صورت میں خود کو کمزور محسوس کرتا ہے کیونکہ ان پر کوئی مسلّط ہو کر ان کو برا محسوس کرانے پر تلا ہوا ہے۔ لہٰذا دوسرا شخص بُلیڈ ہونے پر بھڑک جاتا ہے۔ ہار جیت کا یہ عمل بہت مشکل ہوتا ہے، لیکن ناممکن ہرگز نہیں۔ اس صورت میں پہلا قدم ایسی صورتحال سے اچھی طرح سے آگاہ ہونا ہوتا ہے۔

جب کبھی آپ کو آن لائن بُلیڈ کیا جاتا ہے اور آپ اس کا اظہار کسی اور سے کرتے ہیں تو آگے سے آپ کو کہا جاتا ہے کہ آپ آف

لائن ہو جائیں۔اس کا مطلب یہ ہوا کہ ایک سوشل میڈیا صارف ہونے کے ناتے آپ ان سب باتوں کے خود ذمہ دار ہیں۔ہم اس بات سے متفق ہرگز نہیں اور ایسا کیوں ہے، آئیے بیان کرتے ہیں

ہم اکثر سنتے ہیں:

''آپ پھر بھی آن لائن کیوں ہیں؟''

''آپ اسے بلاک کیوں نہیں کر رہی؟''

''آپ یہ سب پہلے کیوں کہ رہی ہو؟''

''درگزر کریں! ایسے لوگوں کے منہ مت لگیں!''

''اپنا اکاؤنٹ ڈی ایکٹیویٹ کر دیں۔''

''انٹرنیٹ تو ویسے بھی خواتین کیلئے محفوظ نہیں ہے آپ تیہاں کیوں ہو؟''

یہ باتیں نا قابلِ برداشت ہوتی ہیں خصوصاً جب آپ کے جاننے والے آپ کے پیارے ایسا کہیں۔چونکہ وہ ہمیں پریشان ہوتا نہیں دیکھ سکتے لہٰذا ایسی باتوں کا انہیں یہی حل نظر آتا ہے۔

یاد رکھیں:

★ آپ آن لائن ہیں کیونکہ انٹرنیٹ استعمال کرنا آپ کا حق ہے اور جو کوئی آپ کو اس کے استعمال سے روکتا ہے تو بنیادی طور آپ کو آپ کے حق سے دستبردار کرنا چاہتا ہے۔

★ یہ فیصلہ آپ کو کرنا ہے کہ آپ کو کس سے بات کرنی ہے اور کس کو بلاک کرنا ہے۔بعض لوگ مافوق الفطرت لوگوں سے بات شروع کر دیتے ہیں اور بعض دفعہ یہ کام آتی ہے۔اگر آپ کسی کو بلاک کر دیتی ہیں تو وہ نئی پروفائل بنا لیتے ہیں حالانکہ ہم آ بلاک کرنے کی تجویز دیتے ہیں لیکن ساتھ ساتھ ہم خبردار بھی کرتے ہیں کہ یہ مکمّل حل نہیں ہے۔

★ جی ہاں، بعض کمنٹس سے درگزر کر جانا چاہئے لیکن درگزر کرنا مسائل کا حل نہیں ہوتا۔

★ اگر آپ اپنا اکاؤنٹ ڈی ایکٹیویٹ کر دیتے ہیں تو سمجھیں آپکو ٹنگ کرنے والا جیت گیا۔ آپ نے اسے مزید شہ دے دی ہے۔ اب وہ مزید طاقتور ہو گیا ہے اور اسے مزید شہ مل گئی ہے۔ اب وہ سوچے گا کہ وہ ہراساں کرنے سے اپنے مذموم مقاصد حاصل کر سکتا ہے۔

★ کیا عورتوں کیلئے محفوظ جگہ ہے؟ جب عورتوں کیخلاف تشدد کی بات ہوتی ہے تو یقیناً ہم کہیں پر بھی محفوظ نہیں ہیں۔ نہ ہی ہم اپنے گھروں میں محفوظ ہیں، نہ ہی پبلک مقامات پر، اور نہ ہی کام کاج کی جگہ پر۔ کوئی بھی مقام خواتین کیلئے تب تک محفوظ نہیں ہوگا جب تک ہم کسی مقام کا دعوٰی کر کے اسے اپنے لئے محفوظ نہیں بنا لیتی۔

آمنہ ایک بلاگر ہے جو خواتین کے حقوق سے متعلّق کافی کچھ لکھتی رہتی ہے۔ بہت سے لوگ اس کی رائے سے اتفاق نہیں کرتے اور اسے اپنے بلاگ کے جوابی صفحات پر کافی تنقید کا سامنا بھی کرنا پڑتا ہے۔ ان تبصروں میں سے کافی سارے بدخوئی پر مبنی ہوتے ہیں جن میں سے چند مثالیں مندرجہ ذیل ہیں:

★ خود کو مار ڈالو!
★ تم بہت موٹی اور بھدی ہو!
★ تم پاگل اور بیکار ہو!
★ کوئی تمہاری بات سننے کو تیار نہیں!
★ کوئی تمہیں پسند نہیں کرتا!
★ اس کام کیلئے تم جہنّم جاؤ گی!
★ تمہارا آبرو ریزی ہونی چاہئے!
★ میں تمہیں قتل کر دوں گا!
★ میں تمہارے چہرے پر تیزاب پھینک دوں گا!
★ تمہاری زندگی بے مقصد اور بیکار ہے!

بعض تبصرے کافی لمبے، جامع لیکن پریشان کر دینے والے ہوتے ہیں۔ آمنہ کو جب بھی ایسی جسمانی نقصان پہنچانے کی دھمکیاں موصول ہوتیں تو وہ بہت زیادہ پریشان ہو جاتی۔

دراصل آمنہ اس بات سے ناواقف تھی کہ ان تبصروں سے کیسے نبٹنا ہے۔ جب اس نے دوسری خواتین بلاگرز سے اس بات کا تذکرہ کیا تو اسے پتہ چلا کہ یہ سب سہنے والی وہ اکیلی عورت نہیں تھی۔ ان میں سے بعض کو تو بالکل ویسی ہی دھمکیاں اور تبصروں کا سامنا کرنا پڑا۔ خواتین کی اس جماعت نے اس کی مدد کرتے ہوئے اسے ایک ایکٹیوسٹ سے ملایا جو ایسے مسائل سے نبرد آزما ہونا جانتی تھی۔

ان خواتین نے یہ فیصلہ بھی کیا کہ ایک دوسرے کی مدد کرنے کیلئے ایک حمایتی گروپ تشکیل دیا جائے۔ معلوم کرنے پر اسے پتہ چلا کہ جن خواتین کو ایسی نفرت انگیزی کا سامنا کرنا پڑا ان میں سے زیادہ تر خواتین عام حالات سے ذرا ہٹ کر انسانی حقوق کی باتیں کرتی تھیں۔ خواتین صحافیوں اور مصنفین نے اسے بتایا کہ وہ ایسی مافوق الفطرت باتوں کی عادی ہوگئی تھیں اور یہ باتیں اب انہیں زیادہ پریشان نہیں کرتی۔ آمنہ کیلئے یہ بڑی تشویشناک بات تھی۔ کیونکہ انسان کسی اور سے نبرد آزما ہونے کیلئے احساسات سے عاری کیسے ہوسکتا ہے۔

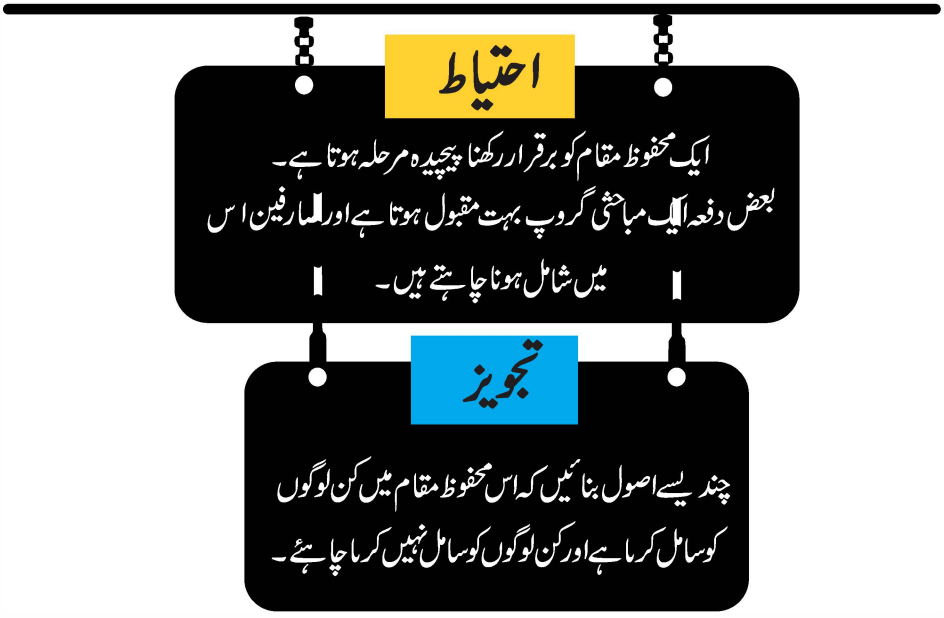
آئینِ پاکستان کی شِق 19 یہ بتاتی ہے کہ ہم 'معقول شرائط کیساتھ'
تقریری آزادی رکھتے ہیں، جس کا مطلب یہ ہوا کہ یہ حق مکمل نہیں ہے۔

#KnowyourRights

آمنہ نے سب سے پہلا قدم یہ اٹھایا کہ اعتدال پسندانہ تبصرے دینے شروع کئے اور کسی بھی نفرت انگیز تبصرے کی حمایت کرنا ترک کردی۔ جب اسے تنگ کرنے والوں کو یہ بات سمجھ آئی کہ وہ ان کی گالیوں کی کوئی پرواہ نہیں کرتی تو انہوں نے اسے تنگ کرنا چھوڑ دیا۔ لیکن ان میں سے ایک نے تبصرے دینا بند نہ کیا۔ اپنے حامی گروپ سے رابطہ کرنے پر اس کی یہ مدد ہوئی کہ اس دھمکی آمیز تبصرہ کرنے والے شخص کی رپورٹ کردی گئی۔ ان تبصروں کو ختم ہونے میں چند ماہ لگ گئے لیکن اب بھی آمنہ کو کبھی کبھار کچھ خوفناک قسم کی ای میلز اور تبصروں کا سامنا کرنا پڑتا ہے۔ اب آمنہ سمجھ چکی ہے کہ ایسے تبصرے اسے خاموش کرانے کیلئے بھیجے جاتے ہیں۔ لیکن اب اس نے اپنی تحریریں بھی جاری کرنا شروع کردی ہیں اور ایسے ہتھکنڈوں کے سامنے ہتھیار پھینکنے سے انکار کردیا ہے اور اب وہ اپنے بُلیز کو جیتنے کا کوئی موقع فراہم نہیں کرتی۔

اسی لئے ہتھیار ڈالنے کی بجائے سائبر پلیٹ فارم جیسے سوشل میڈیا پر رہنا نہایت اہمیت کا حامل ہے۔ اسی لئے ہم محفوظ وسعتیں تشکیل کرنے کی حمایت کرتے ہیں۔

سوشل میڈیا یا ایک میلنگ لسٹ پر ایک نزدیکی گروپ تشکیل دیکر ایک محفوظ جگہ مرتب کی جاسکتی ہے۔ یہ ایک کلوزڈ بلاگ یا ایک فورم بھی ہوسکتا ہے



★ آپ کی روایات کیا ہیں؟ جو انہیں سمجھتے ہیں انہیں شامل ہونا چاہئے۔ اگر کوئی اس سے صرفِ نظر کرتا ہے لیکن وہ انہیں سمجھنا چاہتا ہے تو اس صارف کو اپنے گروپ میں رکھنے کیلئے آپ کو مشاورت کے بعد فیصلہ لینا چاہئے۔

★ سیکھنے اور اپنے نظریات کو چیلنج ہونے پر خندہ پیشانی کا ثبوت دیں۔

★ اپنے گروپ سے معلومات کا باہر آنے اور نوسکرین کیپچرنگ جیسی حکمتِ عملیوں کیساتھ آئیں۔

★ اپنے ان جوازوں کے بارے میں سوچئے جو آپ ان لوگوں کو دیتے ہیں جو دوسروں پر ذاتی حملے کرتے ہیں اور جو کسی کی رازداری کی روگردانی کرتے ہیں۔

★ بحث ومباحثہ زور پکڑتے رہتے ہیں۔ یہ بات تب تک ٹھیک ہے جب تک سب کا احترام کیا جارہا ہو اور دوسروں کے خیالات کو سننے کی کوشش کی جاتی رہی ہو۔ اپنے ذہن کو کشادہ کریں۔

★ جب ایک گفتگو ناگوار صورتِ حال اختیار کر جائے تو اس وقت کیا کرنا چاہئے؟ ان حکمتِ عملیوں سے وابستہ رہیں جو ایک ایسی صورتِ حال سے نمٹنے سے متعلّق ہوں۔

آپ انہی ہدایات پر عمل کریں جو آپ طبعی زندگی میں کریں گی۔ آپ ان مقامات پر جاتی ہیں جہاں آپ خود کو محفوظ سمجھتی ہیں خاص طور پر جب آپ اپنے دوستوں سے ایسی گفتگو کرنی پڑے جو آپ چاہتی ہوں کہ اسے کوئی اور نہ سنے۔ آپ کبھی یہ نہیں چاہیں گی کہ کوئی آپ پہ چلّائے۔ لوگ اس بات کو سمجھتے ہیں کہ انہیں کسی بھی عوامی مقام پر آپ پر حملہ کرنے کی اجازت نہیں ملے گی اس لئے وہ

ایسا کرنے سے ہچکچائیں گے۔پس اس مشق کو روزمرہ کے تجربے کے طور پر کریں: آپ کا آن لائن مقام اتنا ہی اہم ہونا چاہئے جتنا آپ کا آف لائن مقام۔ دونوں مقام ایسے ہونے چاہئیں کہ جہاں آپ بہت کچھ سیکھ بھی سکیں اور اپنے خیالات، جذبات اور احساسات کا اظہار کرسکیں۔ دونوں مقامات آپ کے علم میں اضافہ کریں گے اور کبھی کبھی آپ کو اپنا ذہن بدلنے کی بھی ضرورت پڑے گی ان باتوں کیلئے جن پہ آپ کے خیالات کو چیلنج کیا گیا ہو۔

انٹرنیٹ کو ایک محفوظ مقام پر چلانے کیلئے سب سے بہترین طریقہ یہ ہے کہ آن لائن ہراساں ہوئے لوگوں کے حامی گروپس ایسی جگہ مرتب کریں جہاں وہ ایک دوسرے کی حمایت کر سکتے ہوں۔ آپ کا مرتب کیا ہوا محفوظ مقام ایک ایسا پلیٹ فارم بن سکتا ہے جہاں آپ حامی گروپس مرتب کر سکتے ہیں اور کسی مافوق الفطرت بندے کے حملے سے مل کر نبٹنے کیلئے ایک جگہ ڈٹے رہ سکتے ہیں۔

”ہمارا انٹرنیٹ“ کی تشکیل

ایک ملک کا باشندہ ہونے کے ناتے آپ اپنے ملک کیساتھ ہونے والے سماجی معاہدوں سے باخبر رہتی ہیں۔تاہم انٹرنیٹ کی نہ تو کوئی ریاست ہوتی ہے نہ ہی کوئی حکومت ہوتی ہے اور نہ ہی کوئی ظاہری سماجی معاہدے جیسی کوئی چیز ہوتی ہے۔

یہی وجہ ہے کہ بعض دفعہ انٹرنیٹ ایک تاریک اور ڈراؤنی جگہ بن سکتی ہے۔بنی نوع انسان کی تاریخ میں یہ بات روزِ اول سے پائی جاتی ہے کہ وہ طاقت کا استعمال کرتے ہیں اور طاقت کی خواہش کو بڑھانے کیلئے انسانوں نے بہت سے نئے ہتھیار بنالئے ہیں۔ ہم غذائی تسلل پر بڑی شیخی بگھارتے ہیں۔ہم طاقت رکھنے اور اپنی طاقت کے استعمال پر بہت فخر کرتے ہیں۔

انٹرنیٹ جیسی جدید ٹیکنالوجی بھی ایک طاقت ور حلقہ ہے۔جو اس کے استعمال کی استطاعت رکھ سکتے ہیں وہ اس پہ بہت سی جگہ حاصل کر لیتے ہیں۔جو لوگ اس بات کو اپنا استحقاق سمجھتے ہوئے پوسٹ بھیجتے ہیں انہیں بہت کچھ سننا بھی پڑتا ہے۔جو لوگ مقبول رائے پر تنقید کرتے ہیں ان کی نسبت وہ لوگ زیادہ آسانی سے مقبولیت حاصل کر لیتے ہیں جو ایسی
بات کا زیادہ پرچار کرتے ہیں جو ہر عام انسان سننا چاہتا ہے۔

پاکستان میں خواتین کی نسبت مرد صارفین کی تعداد کافی زیادہ ہے۔سب نہیں لیکن زیادہ تر مرد چاہے آن لائن ہوں یا آف لائن تشدد کا استعمال خواتین یا دوسری غیر محفوظ جماعتوں کو خاموش کرانے کیلئے کرتے ہیں۔ہمارے لئے تو گلیاں بھی محفوظ نہیں رہی، کیونکہ جس جگہ کو اپنی ملکیت سمجھتی ہیں اس میں ہمارے لئے کوئی جگہ نہیں ہوتی۔اسی وجہ سے دفاتر بھی نقصان دہ ہو سکتے ہیں اور پھر ایک کبھی نہ ختم ہونے والی تفصیل موجود ہے۔

یہ کوئی حیرت کی بات نہیں ہے کہ طاقت ور ہر مقام پر اپنی طاقت برقرار رکھنا چاہتا ہے یہی وجہ ہے کہ پسماندہ جماعتوں کے لوگ آن لائن گالیاں کھا کر بس کر دیتے ہیں۔وہ ہم سے تسلیم کروانا چاہتے ہیں کہ ہر جگہ ان کیلئے ہے اور ہم کسی چیز کے بھی دعوے دار نہ ہوں۔ہم جتنی آگے بڑھنے کی کوشش کرتی ہیں اتنا ہی ہمیں ناکامی کا سامنا کرنا پڑتا ہے۔

لیکن یہ کوئی بری خبر نہیں ہے۔ آن لائن مقامات کا انحصار صارفین کے مرتب روئیے پر ہوتا ہے اور ہم بحیثیت صارف اپنی ثقافت کی تشکیل کے ضامن ہوتے ہیں۔ ثقافتیں بدل کر خصوصاً آج کے تیز ترین دور کو مرتب کرتی ہیں۔

آج کے دور کے ضامن ہوتے ہوئے اگر ہمیں انٹرنیٹ کو سب کیلئے محفوظ بنانا ہے تو ابھی فیصلہ کرنا ہے۔ کیا آپ اس دنیا کا تصور کر سکتی ہیں جس میں آن لائن رہ کر لوگ اچھے اخلاق کو فروغ دیں؟

تبدیلی آپ سے شروع ہوتی ہے۔ دوسروں پر انگلی اٹھانا بہت آسان ہوتا ہے اور خود کو مسائل پیدا کرنے کا موجب ٹھہرانا سب سے زیادہ مشکل ہوتا ہے۔ اپنے آپ کو یاد دلاتی رہیں کہ آپ کو سائبر بُلی نہیں کیا جا سکتا اور اس بات پر ڈٹی رہیں کہ سائبر بُلنگ عام ہوگئی ہے اور اسے آن لائن تجربے کے طور پر تسلیم کریں۔ لوگوں اپنی زندگیوں میں سائبر بُلیڈ ہونے کیلئے خود کو تیار رکھیں۔ درحقیقت ایسا ہونا نہیں چاہئے۔

ہمیں انٹرنیٹ کا بہترین باشندہ یا دوسرے لفظوں میں بہترین نیٹیزن بننے کیلئے کچھ قواعد کے ساتھ چلنا پڑے گا۔ مثال کے طور پر ہمیں کوشش کرنی چاہئے کہ ہم آن لائن اپنے غصے کو ہوا نہ دیں۔ ہمیں اس بات کیلئے خبردار رہنا پڑے گا کہ ہمارے اوپر گالیوں کی بوچھاڑ ہوسکتی ہے اور کسی کی جانب سے ہمیں ہدف بنایا جا سکتا ہے محض اس لئے کہ شاید ہمارے لئے وہ ایک برا دن ہو۔ الغرض ہمیں خود کو چوکنا رکھنا چاہئے۔

انسان ایک معاشرتی جانور ہے جو لوگوں کی اس جماعت کیساتھ رہنا پسند کرتا ہے جنہیں وہ سمجھتا ہو کہ اس کی بات سنیں گے۔ اسی لئے ہم اپنے رشتہ داروں اور احباب کو اہمیت دیتے ہیں۔ جب وہ کسی مشکل میں پڑتے ہیں تو ہم ان کی مدد کرتے ہیں کبھی کبھار تو اس وقت بھی مدد کرنی پڑتی ہے جب ہم ان سے اتفاق نہیں کر رہے ہوتے۔

کیا آپ ایک طبعی مقام پر اپنی ایسی سہیلی کی مدد کریں گی جس پر حملہ ہوا ہو؟ ہم یہ تصور کر رہے ہیں کہ آپ اسی وقت اٹھیں اور اس سہیلی کی مدد کریں۔ ہم یہ بھی جانتے ہیں کہ آپ اپنی اس سہیلی کی جگہ یہ جانتے ہوئے خود لڑیں گی کہ اس کے مزید کچھ کہنے سے وہ خود کافی پریشان ہو جائے گی۔

کیا آپ اپنی کسی ایسی سہیلی یا رشتے دار کی مدد کرتی ہیں جسے سائبر بُلیڈ کیا گیا ہو؟ کیا آپ اس کو گالی دینے والے کو منہ توڑ جواب دیتی ہیں؟ کیا آپ اپنے مخالف حریف کو منہ توڑ جواب دینے کی کوشش کرتی ہیں؟

یہاں ہم آپ کو چند بنیادی تجاویز دیتے ہیں جنہیں آپ انٹرنیٹ کو ایک محفوظ مقام بنانے کیلئے استعمال کر سکتی ہیں۔ سب سے پیچیدہ بات یہ ہے کہ آپ آن لائن ایسا رویہ رکھیں
جیسا کہ آپ آف لائن رکھتی ہیں۔

★ آن لائن ہمیشہ ایسے ہی حمایت کریں جیسے آپ آف لائن کرتی ہیں۔ اگر ایک سہیلی کو بُلیڈ کر دیا گیا ہے تو ہمیشہ اس کے ساتھ رہیں اور اس کا مسئلہ حل کرنے میں اس کا ساتھ دیں نا کہ اس سے کنارہ کشی کریں۔

★ بُلیڈ ہونا کسی صورت گوارہ نہ کریں اور بُلیر کیخلاف کھڑے ہو جائیں۔ ''مجھے بُلیڈ کیا جا رہا ہے'' کہنے کی بجائے یہ کہیں ''میں بُلیڈ کبھی نہیں ہوں گی اگرچہ تم ایسا کرنے کی کوشش کر رہے ہو''۔

★ دوسروں کیساتھ نرمی سے پیش آئیں۔ دوسروں کو آپ کی ناپسندیدہ رائے کا اظہار کرنے دیں۔ اسے سنیں اور برسرِ پیکار ہو جائیں۔

★ لوگوں کی پرائیویسی کا خیال رکھیں۔ اگر کوئی آپ پر حاوی ہوتے ہوئے آپ کی پروفائل جاننے کی کوشش کرتا ہے اور آپ کو یہ جان کر برا لگتا ہے تو آپ بھی اسی کی طرح نہ کریں۔

★ جب بھی آپ کوئی معلومات شیئر کرنے لگیں تو خود سے یہ سوالات ضرور کریں کیا یہ معلومات موزوں اور تصدیق شدہ ہیں؟ کیا یہ حقیقت پر مبنی ہیں؟ کیا یہ توہین آمیز ہیں؟ کہیں اس کا مقصد خوف پھیلانا تو نہیں۔ یاد رکھیں کوئی بھی معلومات انٹرنیٹ پر تیزی سے پھیلتی ہیں اسی وجہ سے دھوکہ بازی آسانی سے پھیلتی ہے۔ کیا آپ کسی ایسی ثقافت کا حصہ بننا چاہتی ہیں جس کا مقصد جھوٹی خبروں کو پھیلانا ہو، یا آپ خود کو ایک معتبر ذریعہ بنانا چاہتے ہیں؟ فیصلہ آپ پر ہے۔

★ جب بھی کوئی کام شیئر کریں تو اس کے مصنّف کو ضرور سراہیں۔ ہم اکثر تصاویر کو یہ سوچے بغیر شیئر کر دیتے ہیں کہ اسے کس نے بنایا؟ کس نے اٹھایا ہے؟ اس بات کو ہمیشہ یقینی بنائیں کہ آپ دوسروں کے کئے گئے کام پر اسے ضرور سراہیں گی۔

★ کسی کے الفاظ کی ہو بہو نقل اتار کر انہیں اپنا بنا کر پیش مت کریں بلکہ ایسا کرنے سے پہلے ان الفاظ کے تخلیق کار سے ضرور اجازت لے لیں۔ آپ یونیورسٹی میں کسی قسم کی چوری نہیں کرتے لہٰذا آن لائن بھی ایسا کرنے سے باز رہیں۔

★کسی کی تصویر اس کی رضا مندی کے بغیر اپ لوڈ نہ کریں، ہم اکثر ایسا بغیر اجازت کرتے ہیں اور اس حقیقت سے واقف نہیں ہوتے کہ ان کے کیا نتائج برآمد ہوں گے۔ایسے لوگ جن کی تصاویر آپ بغیر رضا مندی کے بھیج دیتے ہیں ان کیلئے کتنے مسائل کھڑے ہو سکتے ہیں لہٰذا ہمیں ان نتائج سے آگاہ رہنا چاہئے۔رضا مندی بہت اہم ہے۔

★بعض دفعہ لوگ بہت سی اوچھی باتیں بغیر سوچے سمجھے کر جاتے ہیں اور ہم فوری ردِعمل دکھاتے ہوئے اسے ایک انسان ہونے کے ناتے قبول کر لیتے ہی۔تاہم جب ہم ایسا فوری ردِعمل کسی کے سامنے کرتے ہیں تو وہ ہماری جسمانی حرکات اور ہمارے تاثرات جان رہے ہوتے ہیں۔وہ خوفزدہ تو ہو رہے ہوتے ہیں لیکن وہ اس بات سے بھی واقف ہوتے ہیں کہ ان کا کسی کو جج کرنا ٹھیک بات نہیں ہے۔تاہم سائبر سپیس میں ایسا کچھ نہیں ہوتا۔یاد رکھیں سائبر سپیس میں کوئی کسی کی حرکات کو نہیں دیکھ رہا ہوتا۔نہ ہی ہم چہرے دیکھ رہے ہوتے ہیں نہ ہی کسی کی جسمانی حرکات وسکنات کا پتہ چلتا ہے،ہم صرف الفاظ دیکھ رہے ہوتے ہیں اور ہم اپنے جذبات انہیں الفاظ کیساتھ نتھی کر دیتے ہیں۔ہم لوگوں کے ردِعمل پر اپنا ردِعمل دکھاتے ہیں۔ہم انہیں اپنے ہی سانچے سے پرکھ رہے ہوتے ہیں۔ایسا سانچا ہمیشہ متعصّب ہی ہوتا ہے۔ہم کیا کرتے ہیں کہ کوئی سا ایک آرٹیکل یا ٹویٹ کو لیکر یہ فیصلہ کرنا شروع کر دیتے ہیں کہ ہم اسے پسند کریں یا ناپسند۔دوسرے الفاظ میں یوں کہیں تو بے جا نہ ہوگا کہ ہم اپنے آپ میں جج بن جاتے ہیں اور یہ چیز ثقافتی تبدیلی کی راہ میں حائل ہوتی ہے۔اس سے ہٹ کر یہ کیا کریں کہ ردِعمل اور دوسروں کو جج کرنا چھوڑ دیں تا کہ دوسرے آپ کو الفاظ کی بجائے انسان نظر آئیں۔

★کسی بھی مجمع کا حصہ بننا بہت آسان ہوتا ہے۔بعض دفعہ صارفین سوشل میڈیا پر کسی بے ہودہ چیز کو ہاتھوں ہاتھ لیتے ہیں اور اس کا مذاق اڑانا شروع کر دیتے ہیں۔وہ کوئی ایسا آرٹیکل ہو سکتا ہے جو غیر مقبول رائے رکھتا ہو۔نظریہ حقوقِ نسواں جیسے نظریات کو بھی مذاق کے قابل سمجھا جاتا ہے۔یہ بھی ایک قسم کی بُلنگ ہوتی ہے۔جب کسی جماعت کا کوئی رکن یہ سمجھتا ہے کہ انہیں خود کو ظاہر کرنے پر ان کا مذاق اڑایا جائے گا تو وہ اپنے خیالات کا اظہار ہی کرنا چھوڑ دیتے ہیں۔کوشش کریں کہ آپ مسائل کا حصہ نہ بنیں۔بلکہ آگے بڑھ کر اس میں شامل ہو کر مزاحمت کریں اور مسائل کے حل میں اپنا حصہ ڈالیں۔فسادی ذہنوں سے دور رہیں۔

★بہت سے لوگ اپنے تعصّب بھرے ذہن پر مزاح کا پردہ ڈال دیتے ہیں۔ایسے لوگ جنسی قسم کے توہین آمیز لطیفے بناتے ہیں اور مزید جب ان سے کوئی بُلنگ کی شکایت کرتا ہے تو وہ آگے سے مذاق اڑاتے ہیں۔اگر کسی کو یہ اندیشہ ہو کہ ان کا تمسخر اڑایا جائے گا تو پھر وہ اپنی رائے دینے سے ہچکچاتے ہیں۔اگر کسی جماعت کیلئے کوئی لطیفہ توہین آمیز ہوتا ہے چاہے وہ کتنا ہی مزاحیہ ہی کیوں نہ ہو ،اسے شیئر یا اس کی حوصلہ افزائی کبھی نہ کریں کیونکہ یہ بھی تشدد کی ایک شکل ہے جس کا نفسیاتی طور پر استعمال کیا جاتا ہے۔ان

معاملات پر مزاحمت کرنے سے مسائل کھڑے ہو سکتے ہیں۔

★بعض لوگ حفاظتی سکرین کے پیچھے سے دوسروں پر وار کرتے ہیں۔ وہ کوئی ایسی بات کر دیتے ہیں جو بہت تکلیف دہ ہوتی ہے اور خاص طور پر اگر ایسا آپ کے کسی جان پہچان

والے شخص کیساتھ ہو۔ تاہم ایک بات یاد رہے کہ اس اواٹار کے پیچھے ایک انسان موجود ہے جو شاید کسی مشکل وقت سے گزر رہا ہو۔ ایسی باتوں پر ردِعمل دکھانے کی بجائے اس تک پہنچیں۔ اگر وہ اپنی غلطی مان لے تو پھر معاف کرنا بھی سیکھ لیں۔

★اسی طرح اگر آپ کے مزاج میں ناگواری پیدا ہو رہی ہے اور آپ کے غصے کو ابھارا جا رہا ہے تو اپنی ڈیوائس سے کہیں دور چلے جائیں۔ اسے خود سے دور رکھیں۔ باہر گھومنے چلے جائیں اور جب مزاج میں کچھ بہتری آئے تو واپس آن لائن آجائیں۔

★اگر آپ آن لائن اثر و رسوخ رکھتی ہیں تو یاد رہے یہ آپ خصوصی اہمیت کے حامل ہیں ورنہ ہر کسی کو ایسی اہمیت حاصل نہیں ہوتی۔ آپکو ایک طاقتور حیثیت حاصل ہے اور آپ کو یہ فیصلہ کرنا ہے کہ اس طاقت کا استعمال کیسے کرنا ہے۔ آپ اس کا مثبت استعمال کر کے ثقافتی تبدیلی لانے میں مددگار ثابت ہو سکتے ہیں۔ اپنی اس طاقت سے باخبر رہئے اور دانشمندانہ طریقے سے اس کا استعمال کریں۔

ہم امید کرتے ہیں کہ آپ ان تجاویز کو بروئے کار لا سکتی ہیں اور ہمارے ساتھ شامل ہو کر انٹرنیٹ کو ایک محفوظ جگہ بنانا چاہیں گی۔ اگر ہم اپنی مجتمع طاقت کیساتھ کمر کس لیں تو ہم پورے اعتماد کیساتھ ایک مثبت تبدیلی لا سکتی ہیں۔

#OccupyCyberSpace

مختلف ذرائع کی تفصیل

ڈیجیٹل دفاع کیلئے آپکو بہت سی ویب سائٹس مل سکتی ہیں۔ان میں سے چند ایک ہم آپ کیلئے تجویز کرتے ہیں۔

★ Heartmob https://iheartmob.org/

★ Crash Overside https://www.crashoverridenetwork.com/

★ Troll Busters http://www.troll-busters.com/

★ Zen manual

https://gendersec.tacticaltech.org/wiki/index.php/Complete_manual

★ Tactical Tech's Security In A Box https://securityinabox.org/en

HAMARA
INTERNET