ڈیجیٹل وراثت

جائزہ

کیا آپ نے کبھی اس مشکل اور تکلیفدہ سوال کے بارے میں سوچا ہے کہ،»آپ کے مرنے کے بعد یا جب آپ ٹیکنالوجی استعمال کرنے کے قابل نہیں رہیں گے تو آپ کی ڈیجیٹل موجودگی کا کیا بنے گا؟» ہم میں سے کئی لوگوں کے پاس پہلے سے وصیت اور ایسی فہرست موجود ہو گی یا ہونی چاہیئے جس میں وہ تمام باتیں لکھی ہوں جن کے بارے میں آپ چاہتے ہیں کہ آپ کے پیاروں کو آپ کے اس دنیا سے جانے کے بعد علم ہو- لیکن ہماری ڈیجیٹل معلومات اور ڈیجیٹل اکاؤنٹس کا کیا بنے گا؟ کیا ہمیں کسی قسم کی ڈیجیٹل وصیت کے بارے میں سوچنا چاہیئے؟ کیا ہمیں «ڈیجیٹل وراثت» کا منصوبہ بنانا چاہیئے؟

آپ اپنی ڈیجیٹل موجودگی کے بارے میں سوچیں- بینک اور ریٹائرمنٹ اکاؤنٹس، گھر کے لیئے قرضے، خاندان کی تصاویر اور ویڈیوز، اسمارٹ ہوم اکاؤنٹس، ای میل اور سوشل میڈیا آپ کے ڈیجیٹل وجود کی چند مثالیں ہیں- آپ کی یا آپ کے خاندان کے کسی قریبی فرد کی وفات کی صورت میں آپ کے خاندان یا پیاروں کو فوری طور پر ان اکاؤنٹس یا معلومات تک رسائی کی ضرورت پڑ سکتی ہے- مزید یہ کہ پرانی معلومات اور آن لائن اکاؤنٹس میں وقت کے ساتھ ساتھ کمزوریاں رونما ہو سکتی ہیں اور وہ ہیکرز کا نشانہ بن سکتی ہیں جس کی وجہ سے وفات پانے والے شخص کا خاندان اور دوست خطرے میں پڑ سکتے ہیں-

منصوبہ بنانا

بہتر ہو گا کہ آپ اپنی خواہشات، جیسے کہ مرنے کے بعد کی تفصیلات، کا اظہار قابل بھروسہ خاندان کے افراد یا دوستوں سے کریں- اس کے علاوہ آپ اپنے تمام ڈیجیٹل اثاثوں اور آن لائن اکاؤنٹس کی فہرست تیار کریں- اگر آپ اپنے خاندان کے افراد کو اپنے اکاؤنٹس تک رسائی فراہم نہیں کرتے ہیں تو آپ کے مرنے کے بعد ان کے لیئے آپ کے اکاؤنٹس تک رسائی حاصل کرنا یا اسے بند کرنا بہت مشکل ہو سکتا ہے- مثال کے طور پر کیا آپ یہ چاہیں گے کہ آپ کے گھر والے آپ کی ان تمام تصاویر اور ویڈیوز سے محروم ہو جائیں جنہیں آپ نے پچھلے کئی سالوں میں اپلوڈ کیا تھا؟

اس کا ایک طریقہ یہ ہے کہ آپ اپنی تمام آن لائن معلومات کا اندراج ایک پاس ورڈ مینیجر میں کریں- یہ ایک ایسا پروگرام ہے جو آپ کے تمام لاگ اِنز اور پاس ورڈز، کریڈٹ کارڈز اور دوسری حسّاس معلومات کو محفوظ طریقے سے ذخیرہ کرتا ہے- اس پروگرام کو خاص طور پر پاس ورڈز اور سکیورٹی سوالوں کو نہایت آسان طریقے سے بنانے، اُسے ذخیرہ کرنے اور اُس تک رسائی حاصل کرنے کے لیئے تخلیق کیا گیا ہے- یہ کئی طرح سے ایک بہت طاقتور ٹُول ہے جو آپ کی ڈیجیٹل موجودگی کی فہرست کو ذخیرہ کرنے کے لیئے استعمال ہوتا ہے- کئی ایسے پاس ورڈ مینیجرز بھی موجود ہیں جنہیں آپ کنفیگر کر کے اپنے تمام یا کچھ مخصوص پاس ورڈز کو اپنے خاندان کے قابل بھروسہ افراد کے ساتھ اشتراک کر سکتے ہیں- اگر آپ ایسا کرنے پر غیر آرامدہ محسوس کر رہے ہیں تو آپ پاس ورڈ مینیجر تک رسائی کی معلومات لکھ کر ایک لفافہ میں بند کر دیں اور پھر آپ کی وفات کے بعد اس بند لفافہ کو آپ کا نامزد کردہ کوئی بھی شخص یا آپ کے خاندان کا فرد اسے کھول لے- اس طرح انہیں آپ کے پاس ورڈ مینیجر تک رسائی مل جائے گی اور وہ آپ کے اکاؤنٹس اور ان میں موجود معلومات تک رسائی حاصل کر سکیں گے-

اس کے علاوہ کچھ ایسی ویب سائٹس بھی ہیں جو آپ کو اپنے قابل اعتماد رابطوں کی نشاندہی کرنے کا اختیار دیتی ہیں- مثال کے طور پر فیس بک اپنے صارفین کو پہلے سے یہ اختیار فراہم کرتا ہے کہ اُن کی وفات کی صورت میں ان کا اکاؤنٹ آیا ختم کر دیا جائے گا یا وہ یادگار کے طور پر رکھا جائے گا- اکاؤنٹ کو یادگار (Memorialize) بنانے سے یہ ہوتا ہے کہ وہ صرف آپ کے موجودہ دوستوں کو نظر آتا ہے اور وہاں پر پرانی یادوں کا اشتراک کیا جا سکتا ہے- آخری بات یہ کہ آپ کسی وکیل یا اسٹیٹ منصوبہ ساز (وہ شخص جو آپ کی زندگی میں آپ کی وفات کے بعد آپ کی جائیداد کی تقسیم کی منصوبہ سازی کرتا ہے) سے بات کرنے پر غور کریں جو کہ ڈیجیٹل وراثت پر مہارت رکھتا ہو-

ڈیجیٹل اثاثوں کا وراثت میں ملنا

ہو سکتا ہے کہ آپ اپنے آپ کو کسی ایسی صورت حال میں پائیں جس میں آپ کو حال ہی میں فوت ہوئے اپنے کسی دوست یا خاندان کے فرد کے آن لائن اکاؤنٹس تک رسائی حاصل کرنی ہو یا اس کا پاس ورڈ بازیاب کرانا ہو- ہمارا مشورہ ہے کہ آپ کوئی بھی ایسا قدم اٹھانے سے پہلے ایک وکیل اور خاندان کے دوسرے افراد سے مشورہ کر لیں- کیونکہ ہو سکتا ہے کہ خاندان کے دوسرے افراد آپ کے اس قدم کو دیکھ کر ناراض ہو جائیں-

آپ اس کی ابتداء کسی بھی پاس ورڈ کی شناخت سے کر سکتے ہیں جسے آپ ڈھونڈ سکیں- کیا آپ کے خاندان کے اس فرد نے پاس ورڈ کہیں لکھ کے رکھے ہیں یا اسے کہیں ذخیرہ کیا ہے؟ اگر یہ ممکن نہیں ہو تو پھر آپ یہ دیکھیں کہ آیا آپ ان کے زیر استعمال کسی کمپیوٹر یا موبائل آلات تک رسائی حاصل کر سکتے ہیں اور کیا وہ اس میں ابھی تک لاگ ان ہیں؟ اگر ایسا ممکن نہیں ہے تو پھر آپ کو ہر ویب سائٹ تک رسائی حاصل کر کے فوت ہوئے خاندان کے فرد کے اکاؤنٹ تک رسائی حاصل کرنی پڑے گی- اس طریقے میں اکثر آپ کو ڈیتھ سرٹیفیکیٹ اور اس بات کا ثبوت دینا پڑتا ہے کہ آپ اس شخص کے براہ راست رشتہ دار ہیں- کچھ صورتوں میں آپ اکاؤنٹ تک رسائی یا اس میں موجود معلومات تک رسائی حاصل نہیں کر سکیں گے بلکہ آپ صرف ان معلومات کو حذف کر سکیں گے- ہر ویب سائٹ کا اس طرح کی صورتحال سے نمٹنے کا طریقہ کار مختلف ہوتا ہے اور اس عمل میں کافی وقت بھی درکار ہو سکتا ہے-

آج کی ڈیجیٹل دنیا میں ہمیں مستقبل کی اسٹیٹ منصوبہ سازی کرتے وقت صرف فزیکل اثاثوں کے بارے میں نہیں سوچنا چاہیئے بلکہ ڈیجیٹل اثاثوں کے بارے میں بھی سوچنا چاہیئے-

اردو ایڈیشن

Rewterz پاکستان کی معروف انفارمیشن سکیورٹی کمپنی ہے جو پچھلے سات سالوں سے آئی ٹی سکیورٹی کے شعبے میں خدمات سرانجام دے رہی ہے - کمپنی کے بارے میں مزید معلومات کے لئے http://www.rewterz.com کا دورہ کریں یاہمارے فیس بک پیج https://www.facebook.com/Rewterz کو 'لائک' کریں یا ٹوئیٹر @Rewterz پر فالو کریں-

مہمان مُدیر

شیریل کانلی فشنگ اور آگاہی پر مہارت رکھتی ہیں اور ان کے تجربوں میں لاک ہیڈ مارٹن میں فشنگ پروگرام بنانا اور چلانا شامل ہے- اب وہ SANS کی سیکورٹی آگاہی ٹیم کی مدد کرتی ہیں اور ان کے پاس SSAP (SANS Security Awareness Professional) سرٹیفیکیشن ہے-

وسائل:

پاس ورڈ مینیجرز: http://www.sans.org/u/Y5Y

پاس ورڈز کو آسان بنانا: http://www.sans.org/u/Y63

OUCH! کی اشاعت SANS Security Awareness Program کے ذریعے ہوتی ہے اور اسے Creative Commons BY-NC-ND 4.0 License کے تحت تقسیم کرنے کی اجازت ہوتی ہے۔
آپ اس نیوز لیٹر کو تقسیم کر سکتے ہیں اگر آپ اس کا حوالہ دیں ، اس میں کوئی تبدیلی نہ کریں اور نہ ہی اسے تجارتی مقاصد کے لئے استعمال کریں ۔ ترجمے اور مزید معلومات کے لئے
www.sans.org/security-awareness/ouch-newsletter پر رابطہ کریں. ایڈیٹوریل بورڈ: Walt Scrivens, Phil Hoffman, Alan Waggoner, Cheryl Conley۔ | ترجمہ: شعیب ہاشمی