دسمبر ۲۰۱۶ OUCH!

تمام لوگوں کے لیئے ماہانہ سکیورٹی آگاہی کا نیوزلیٹر

OUCH!

اس شمارے میں شامل ہے:

- آپ کی معلومات
- اپنے آلہ کو وائپ کرنا
- سِم / اسٹوریج کارڈز

محفوظ طریقے سے اپنے موبائل آلات کو تلف کرنا

جائزہ

موبائل آلات جیسے کہ اسمارٹ فونز، اسمارٹ واچز اور ٹیبلیٹس میں بہت حیرت انگیز تیزی کے ساتھ جدّت آتی جا رہی ہے- نتجتاً کچھ لوگ اپنے موبائل آلات بہت تیزی سے تبدیل کرتے ہیں، تقریباً ہر سال- بدقسمتی سے لوگوں کی اکثریت یہ بات سوچے بغیر اپنے آلات تلف کر دیتی ہے کہ اُس میں اُن کی کتنی ذاتی معلومات ذخیرہ ہوئی ہوئی ہیں- اس نیوز لیٹر میں ہم یہ بتائیں گے کہ آپ کے موبائل آلہ میں کتنی طرح کی ذاتی معلومات شامل ہو سکتی ہیں اور آپ اُسے تلف یا واپس کرنے سے پہلے کیسے محفوظ طریقے سے وائپ کر سکتے ہیں- اگر آپ کا موبائل آلہ آپ کے آجر کی جانب سے مُہیّا کیا گیا ہے یا اُس میں آپ کی تنظیم کی معلومات ذخیرہ ہوئی ہیں تو آپ اپنے سُپروائزر سے آلات کے باقاعدہ بیک-اپ اور اُسے تلف کرنے سے متعلق طریقہ کار کے بارے میں پوچھیں اور پھر مُندرجہ ذیل اقدامات پر عمل درآمد کریں:

مہمان ایڈیٹر

ہیتھر مہالک (**@HeatherMahalik**; **+HMahalik**) ManTech CARD میں مرکزی فارنزک سائنسدان ہیں جو کہ فارنزک کے شعبے کی سربراہی کرتی ہیں- وہ SANS Institute کے کورس (Advanced Smartphone Forensics FOR585) کی شریک مُصنّفہ اور کورس لیڈ ہیں اور (Windows Forensic Analysis FOR408) کورس کی انسٹرکٹر بھی ہیں- وہ **smarterforensics.com** پر بلاگ کرتی ہیں-

آپ کی معلومات

موبائل آلات آپ کی سوچ سے زیادہ حسّاس معلومات ذخیرہ کرتے ہیں، اکثر آپ کے کمپیوٹر سے بھی زیادہ- ان میں مندرجہ ذیل مخصُوص معلومات شامل ہو سکتی ہیں:

- آپ کہاں رہتے ہیں، کہاں کام کرتے ہیں اور کِن جگہوں کے کثرت سے دورے کرتے ہیں؟
- آپ کی ایڈریس بُک اور ایپلیکیشنز میں سے تمام لوگوں بشمول آپ کے خاندان، دوستوں اور ساتھ کام کرنے والے لوگوں سے رابطے کی تفصیلات-
- کال ہسٹری بشمول آنےوالی، جانے والی اور مِسڈ کالز-
- SMS (ٹیکسٹنگ)، وائس اور ملٹی میڈیا میسیجز-
- ایپلیکیشنز میں موجود چیٹ سیشنز جیسے سکیور چیٹ، گیمز اور سوشل میڈیا-
- GPS کوآرڈینیٹس کی بنیاد پر لوکیشن ہسٹری یا سیل ٹاور کی ہسٹری-
- ویب براؤزنگ ہسٹری، سرچ ہسٹری، کوکیز اور کیشیڈ پیجز-
- ذاتی تصاویر، ویڈیوز، آڈیو ریکارڈنگز اور ای-میلز-
- ذخیرہ کئے ہوئے پاس ورڈز اور ذاتی اکاؤنٹس تک رسائی، جیسے کہ آپ کا آن-لائن اکاؤنٹ یا ای میل اکاؤنٹ-
- کلاؤڈ پر ذخیرہ کی ہوئی تصاویر، فائلز یا معلومات تک رسائی-
- صحت سے مُتعلّق معلومات بشمول آپ کی عُمر، دل کی دھڑکن کی رفتار، بلڈ پریشر یا ڈائٹ-

محفوظ طریقے سے اپنے موبائل آلات کو تلف کرنا

اپنے آلہ کو وائپ کرنا

جیسے کہ آپ دیکھ سکتے ہیں کہ آپ کے موبائل آلہ میں کہیں زیادہ حسّاس معلومات ہو سکتی ہیں- اس بات سے قطع نظر کہ آپ اپنے موبائل آلہ کو کس طرح تلف کرتے ہیں، جیسے کہ اسے عطیہ کرتے ہیں، کسی نئے آلہ سے تبادلہ کرتے ہیں، خاندان کے کسی دوسرے فرد کو دیتے ہیں، پھر سے بیچتے ہیں یا چاہے پھینک دیتے ہیں، آپ کو اس بات کو یقینی بنانا ہے کہ آپ نے اُس میں سے تمام حسّاس معلومات کو تلف کر دیا ہے- آپ کو شاید اس بات کا احساس نہ ہو لیکن صرف اپنی معلومات کو تلف کرنا بی کافی نہیں ہے کیونکہ یہ انٹرنیٹ پر موجود ٹولز کے ذریعے دوبارہ نکالی جا سکتی ہیں- اس کے بجائے آپ کو اپنے آلہ میں موجود معلومات کو محفوظ طریقے سے تلف کرنا چاہیئے، جو کہ وائپنگ کہلاتا ہے- یہ درحقیقت آپ کی معلومات کو اوور-رائٹ کر دیتا ہے اور اس بات کو یقینی بناتا ہے کہ یہ دوبارہ بازیاب نہ ہو سکے یا یہ ناقابلِ بازیاب ہو جائے- یاد رہے کہ آپ اپنی تمام معلومات وائپ کرنے سے پہلے اُس کا بیک-اپ ضرور لے لیں، اِس طرح آپ اپنے نئے آلہ کی تعمیر نو آسانی سے کر سکتے ہیں-

اپنے موبائل آلہ کو تلف کرتے وقت اِس بات کی یقین دہانی کر لیں کہ آپ نے اُس میں ‹فیکٹری ری-سیٹ› کر دیا ہے اور اگر اُس میں سِم اور SD کارڈز موجود ہیں تو اُنہیں نکال دیا ہے-

اپنے آلہ کو وائپ کرنے کا سب سے آسان ترین طریقہ اُس کے «فیکٹری ری-سیٹ» فنکشن کو استعمال کرنا ہے- یہ آپ کے آلہ کو اُس حالت میں واپس لے آئے گا جس میں آپ نے اُسے خریدا تھا- ہمیں پتہ چلا ہے کہ فیکٹری ری-سیٹ آپ کے موبائل آلات میں سے معلومات تلف کرنے کا سب سے محفوظ اور آسان ترین طریقہ ہے- فیکٹری ری-سیٹ کا فنکشن مختلف آلات میں مختلف ہوتا ہے؛ مندرجہ ذیل اقدامات دو مشہور ترین آلات سے متعلّق ہیں:

- ایپل iOS آلات: Settings > General > Reset > Erase All Content and Settings
- اینڈرائڈ آلات: Settings > Privacy > Factory Data Reset

بدقسمتی سے ونڈوز فون کے آلات میں ذاتی معلومات کو تلف کرنا فیکٹری ری-سیٹ جتنا آسان نہیں ہے- اپنی معلومات کو بحفاظت تلف کرنے کے طریقوں پر مزید تحقیق ہو رہی ہے- اگر آپ کے پاس ابھی بھی فیکٹری ری-سیٹ سے مُتعلّق سوالات ہیں تو آپ اپنے آلہ کے ‹اونر مین-ول› یا مینوفیکچرر کی ویب سائٹ سے رُجوع کریں- یاد رہے کہ اپنی ذاتی معلومات کو تلف کرنا ہی کافی نہیں ہے کیونکہ یہ باآسانی دوبارہ نکالی جا سکتی ہیں-

سِم اور اِکسٹرنل (بیرونی) کارڈز

آپ کے آلہ میں موجود معلومات کے علاوہ آپ کو اس بات پر بھی غور کرنا چاہیئے کہ آپ کو اپنے SIM (Subscriber Identity Module) کارڈ کے ساتھ کیا کرنا ہے- سِم کارڈ موبائل آلات میں سیلولر یا ڈیٹا کنکشن بنانے کے لیئے استعمال ہوتا ہے- جب آپ اپنے آلہ کو فیکٹری ری-سیٹ کرتے ہیں تو سِم کارڈ میں آپ کے اکاؤنٹ سے مُتعلّق معلومات ویسی کی ویسی موجود رہتی ہیں- اگر آپ اپنا نمبر برقرار رکھتے ہوئے نئے آلہ پر مُنتقل ہو رہے ہیں تو اپنی فون سروس فراہم کرنے والی کمپنی سے سِم کارڈ کو نئے آلہ میں منتقل کرنے کی بات کریں- اگر یہ مُمکن نہ ہو، مثال کے طور پر آپ کے نئے فوُن میں مُختلف ناپ کا سِم کارڈ استعمال ہوتا ہے تو آپ اپنے پُرانے سِم کارڈ کو خوُد ٹُکڑے ٹُکڑے کر دیں یا تباہ کر دیں تاکہ کوئی اور اُسے استعمال نہ کر سکے-

محفوظ طریقے سے اپنے موبائل آلات کو تلف کرنا

آخر میں یہ کہ کُچھ موبائل آلات میں مزید اسٹوریج کے لیۓ الگ سے SD (Secure Digital) کارڈ کا استعمال ہوتا ہے- ان اسٹوریج کارڈز میں اکثر تصاویر، اسمارٹ فون ایپلیکیشنز اور حسّاس مواد شامل ہوتی ہیں- اپنا موبائل آلہ تلف کرنے سے پہلے اُس میں سے بیرونی اسٹوریج کارڈز نکالنا نہ بُھولیں (کُچھ آلات میں SD کارڈز بیٹری والے خانے میں چُھپے ہوتے ہیں، مُمکنہ طور پر بیٹری کے نیچے)- یہ کارڈز اکثر نۓ موبائل آلات میں پھر سے استعمال ہو سکتے ہیں یا عام اسٹوریج کے طور پر آپ کے کمپیوٹر یا ‹یوایس بی› ایڈاپٹر میں استعمال ہو سکتے ہیں- اگر SD کارڈ کا دوبارہ استعمال مُمکن نہ ہو تو ہمارا مشورہ ہے کہ آپ اپنے پُرانے سِم کارڈ کی طرح اُسے خُود تباہ کر دیں-

اگر آپ کو اِس نیوزلیٹر میں بتائۓ گئے اِقدامات سمجھ میں نہیں آۓ ہیں تو آپ اپنے موبائل آلہ کو اُس دُکان پر لے جائیں جہاں سے آپ نے اُسے خریدا تھا اور وہاں موجود تربیت یافتہ ٹیکنیشن سے مدد طلب کریں- آخر میں یہ کہ اگر آپ اپنا موبائل آلہ پھینک رہے ہیں تو ہمارا مشورہ ہے کہ آپ اُسے کسی کو عطیہ کر دیں- کئی بہت زبردست خیراتی تنظیمیں استعمال شدہ موبائل آلات کا عطیہ قبول کرتی ہیں-

مزید جانیئے

OUCH! کے ماہانہ سیکیورٹی تعلیم کے نیوز لیٹر کو سبسکرائب کریں،OUCH! archives تک رسائی حاصل کریں اورSANS سیکیورٹی سے مزیدآگاہی کے لئے اس ویب سائٹ کا دورہ کریں securingthehuman.sans.org/ouch/archives (انگریزی میں) ۔

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۔

وسائل:

اپنے نۓ ٹیبلٹ کو محفوظ بنانا: https://securingthehuman.sans.org/ouch/2016#january2016

بیک-اپ اور ریکوَری: https://securingthehuman.sans.org/ouch/2015#august2015

ایڈوانسڈ اسمارٹ فون فارنزک کورس: https://sans.org/for585

OUCH نیوز لیٹر آرکائیوز: https://securingthehuman.sans.org/ouch/archives

ایڈیٹوریل بورڈ: بل وے مین، والٹ اسکریونز، فل ہوفمن، لینس اسپڑنر، کارمن رولی ہارڈی، چیرل کونلی۔

ترجمہ: شعیب ہاشمی