WE ARE GOING TO PITCH OUR NUMBER ALONG. IT'S NOT ZERO. IT'S NOT LIKE GAZILLION PEOPLE AS TO HOW MANY PEOPLE HAVE EXPERIENCED MALICIOUS APPS. JUST BY WAY OF BACKGROUND SOME OF YOU MIGHT BE FAMILIAR WITH OUR STATE OF THE NET SURVEY WHICH WE'VE BEEN DOING ALMOST A DECADE. THOSE ARE SOME OF THE SAMPLES UP THERE.

COUPLE OF YEAR AGO THIS SURVEY FOUND, FOR EXAMPLE, LIKE MILLIONS OF FACEBOOK, UNDERAGE KIDS ON FACEBOOK. WE'VE BEEN TRACKING MALWARE ON COMPUTERS ALMOST TEN YEARS. SAME PEOPLE THAT DO OUR ANNUAL QUESTIONNAIRE DO THIS SURVEY. I HIT THE END BUTTON.

GET ME BACK.

BE CAREFUL WHICH BUTTON YOU TOUCH.

LET'S GET IN TO SOME OF OUR FINDINGS.

THOSE ARE SOME OF THE AREAS THAT WE LOOKED IN TO, MALICIOUS SOFTWARE, STOLEN AND LOST PHONES, LOCATION-TRACKING RISKS, I KNOW PEOPLE THINK OF IT AS PRIVACY ISSUE. WE FOUND SOME DATA. WHERE IT'S A SECURITY ISSUE. THE USE OF INSECURE HOT SPOTS AND HOW CONSUMERS ARE OR ARE NOT SECURING THEIR PHONES. HERE ARE NUMBERS, THIS IS BASED ON ACTUALLY ASKING PEOPLE HOW MANY TIMES MALICIOUS APP HAS
BEEN INSTALLED ON THEIR OWN IN THE PAST YEAR.
WE GAVE THEM CALL PEARLS, SYMPTOMS, UNAUTHORIZED CALLS OR TEXTS.
THAT HEIGHT BE HIGHER THAN 2% IN THE SAME BALLPARK BUT WAY HIGHER THAN -- WE ALSO ASKED PEOPLE HOW THE MALICIOUS SOFTWARE AFFECTED THEM YOU CAN SEE WHAT HAPPENED TO THEM.
THIS WAS A VERY SMALL SAMPLE SIZE BECAUSE OF THE LOW INCIDENTS SO THESE PERCENTAGES ARE PERCENTAGE OF THE PEOPLE WHO HAD MALICIOUS SOFTWARE AND THE MOST COMMON -- I THINK BETTER TO LOOK WHICH ARE BIGGER LINES AND SMALLER LINES THAN TO GET CAUGHT UP IN THE NUMBERS.
RESETTING THE PHONES, HAVING PROBLEMS WERE THE MOST COMMON. TOLL FRAUD, LOSING STUFF ON YOUR PHONE, THERE WAS SOME EXAMPLES OF PEOPLE BEING HARASSED OR I.D. THEFT.
AND SMALL PERCENTAGE OF PEOPLE HAD TO DEACTIVATE THEIR WIRELESS ACCOUNT.
WE ALSO ASKED ABOUT WHAT WE CALL IMPOSTOR APPS WHICH ARE -- REPACKAGED APPS ARE APPS THAT ARE MADE TO LOOK LIKE BRAND NAME APPS.
WE ASKED PEOPLE HOW MANY BRAND NAME APPS THEY DOWNLOADED THAT TURNED OUT TO BE ACTUALLY MALICIOUS IMPOSTOR.
WE PROJECT THAT 1.6 MILLION USERS INSTALL THOSE LAST YEAR.
I KNOW SOME PEOPLE THAT HIVE TALKED TO ARE SKEPTICAL ABOUT THIS.
IF YOU TAKE A LOOK AT THE APP STORES, I DON'T KNOW IF YOU CAN READ FINE PRINT ON HERE, WE
VISITED SOME OF THE -- THESE ARE
MAJOR APP STORES, FOUND IN MAJOR
APP STORES NOT LITTLE ONES WE'VE
BEEN TALKING ABOUT.
THIS DROP BOX LOOK ALIKE HAS
DISCLAIMER THAT I CIRCLED THAT
SAYS APPLICATION IS NOT
AFFILIATED WITH DROPBOX.
BUT THAT LITTLE DISCLAIMER
doesn't show up unless you click
"-- UNLESS YOU CLICK "SHOW
DETAILS" IT IS OF THE ORIGINAL
APP AND THEN OTHER LOGOS ARE FOR
THINGS THAT ARE KIND OF LOOKING
A LOT LIKE THEM.
I'M NOT SAYING THESE ARE
MALICIOUS BUT YOU CAN SEE HOW
CONSUMERS MIGHT NOT BE ABLE TO
tell the real thing from
something else.
looking at phone left and loss.
we just announced this yesterday
that we projected 1.6 million
smartphones were stolen last
year.
Another 1.2 million were lost
and not recovered which is a
security problem not as much as
stolen phone but if you lose
your phone, somebody could still
get at your information.
this were some of the things
that people experienced as a
result of a phone left,
unauthorized access to their
bank account or e-mail account
and permanent loss of photos.
as you see the note there there
was such a small number of
people that we can't give
numbers for these.
then we asked people, what they
were doing to protect their
phone.
of all the measures that we
asked about the winner is over
THERE ON THE RIGHT WHICH IS NONE OF THE ABOVE.
AT 40% OF PEOPLE THAT WAS KIND OF OUR BIG NEWS WHEN WE FIRST RAN THIS STORY.
PROBABLY MOST COMMON PROCESS PEOPLE ARE BACKING UP ABOUT ONE-THIRD ARE BACKING UP AND FOUR DIGIT PASS CODES AND LONGER PASS CODES TOGETHER ARE ABOUT 36%, 23 AND 1 ON THERE.
STILL MAJORITY OF PEOPLE ARE NOT USING PASS CODES.
LOTS OF PEOPLE I'VE SPOKEN TO DIDN'T KNOW YOU CAN USE PASS CODE LONGER THAN FOUR DIGITS, OH, YOU CAN DO THAT?
THERE'S A LOT OF -- LACK OF CONSUMER EDUCATION HERE THAT I THINK IS LOT OF WORK TO CUT OUT.
I THINK THERE'S LOT OF ROOM FOR GROWTH FOR THE ANTI-VIRUS MAKERS THAT ARE HERE, ONLY 15% RIGHT NOW ARE USING ANTI-VIRUS.
MAYBE BECAUSE THEY THINK THEY DON'T NEED IT.
OUR SURVEY OF PC USERS OVER THE LAST TEN YEARS SHOW THAT SOMETHING LIKE IN EXCESS OF -- 80-90% ARE USING ANTI-VIRUS.
THIS IS CLEARLY WAY LOWER THAN WE FIND ON DESKTOP COMPUTERS.
COUPLE OF OTHER THINGS, ONE IS THAT THE FOUR DIGIT PASS CODE NOT ALL IT'S CRACKED UP TO BE. PROPERLY EQUIPPED YOU CAN CRACK IT IN 20 MINUTES.
CONSUMERS, LACK OF TRANSPARENCY IN APP STORES.
CONSUMERS CAN'T TELL WHEN THEY LOOK AT APPS IN THE STORE OR RUNNING THEM WHERE THEY SECURE THE TRANSMISSIONS.
IF YOU GO TO STARBUCKS OR THE AIRPORT OR HOTEL, TENS OF MILLIONS OF PEOPLE DO USE THEIR
APPS THERE YOU CAN'T ALWAYS TELL IF IT'S ENCRYPTING YOUR WIRELESS TRANSMISSIONS.
ALSO THE LAST POINT HERE THAT APP DEVELOPERS VARY A LOT.
WE TALKED TO PEOPLE THAT TOLD US THAT VERY LITTLE TO PROTECT THE DATA THEY STORE ON YOUR PHONE IN THE EVENT THAT IT'S STOLEN OR LOST.
WHERE AS FACEBOOK I'M SURE ARE DOING EVERYTHING THAT APPLE OR GOOGLE PROVIDE THEM WITH.
BUT THERE'S NO WAY THAT YOU AS CONSUMER CAN TELL THE DIFFERENCE BETWEEN A DEVELOPER THAT'S DOING THAT AND DEVELOPER, IS THAT REALLY AREN'T PROTECTING.
WE THINK THERE IS NEED FOR MORE TRANSPARENCY.
IT'S REALLY WORTH READING, I HAVE A LITTLE PICTURE -- PITCH FOR MAGAZINE STORE, THE WHOLE THING IS ON THE WEB FOR FREE.
WE HAVE TUTORIALS FOR PEOPLE HOW TO SECURE THEIR PHONES.
THERE'S A LOT MORE DETAIL THERE INCLUDING HOW MANY APPLE USERS HAVE GONE OUT OF THE APPLE APP STORE.
I'LL LET YOU READ THE STORY TO FIND THAT OUT.

>> GREAT, THANK YOU, JEFF.
I ADDED UP SOME OF THE NUMBERS ON YOUR SLIDES LOOKS LIKE 64% OF CONSUMERS DON'T HAVE PASSWORDS ON THEIR OWN AT ALL.
I CAN SAY FROM EXPERIENCE THAT MY 9-YEAR-OLD HAD TO TELL ME WHEN I FIRST GOT MY SMARTPHONE THAT I COULD DO MORE THAN FOUR DIGIT PASS CODE.
NOW, MARKUS JAKOBSSON HAS PUT A LOT OF THOUGHT IN TO THE VULNERABILITIES OF PASSWORDS.
CAN YOU PLEASE TELL US YOUR
THOUGHTS WHAT YOU ENVISION
ALTERNATIVES COULD BE.
>>  LET ME JUST START BY
COMMENTING ON ONE OF THE NUMBERS
THAT JEFF GAVE.
I THINK SURVEY IS GREAT.
IT'S ONE RISK THAT YOU'RE FACING
WHEN YOU'RE ASKING PEOPLE WHAT
THEY'RE DOING THAT MAYBE THEY
DON'T KNOW WHAT THEY'RE DOING.
WHEN CORPORATIONS MEASURE HOW
MUCH TO WHAT EXTENT MALWARE
PRODUCTS ARE DEPLOYED THEY DON'T
SEE 80% WE SEE MUCH SMALLER
NUMBERS.
IT MIGHT BE BECAUSE PEOPLE THINK
THEY HAVE ANTI-VIRUS PROTECTION
BECAUSE THEY ONCE DID NOW IT
EXPIRED.
OR THEY THINK THAT THEY DID BUT
IT WAS REALLY SOMETHING ELSE.
MANY PEOPLE INSTALL WHAT THEY
BELIEVE IS FREE ANTI-VIRUS AND
IT'S REALLY MALWARE.
THIS IS NOT TO CALL IN TO
QUESTION THE NUMBERS, JUST TO
HIGHLIGHT THE RISK OF ASKING THE
END USER.
IN MY PRESENTATION HERE I WILL
SPEAK ABOUT THE END USER BUT
FROM A DIFFERENT PERSPECTIVE.
I'LL TALK ABOUT PASSWORDS AND
WHY I THINK IT'S GREAT PROBLEM
ON HANDSETS.
ONE OF THE FOREMOST ISSUES IS
THAT IT'S very HARD TO ENTER A
PASSWORD.
A GOOD PASSWORD ON A HAND SET.
AND ALSO THE NUMBER OF
APPLICATIONS AND OPPORTUNITIES
TO AUTHENTICATE THAT PEOPLE
INTERACT WITH ON HANDSETS ARE
GREATER THAN THE DESKTOP MARKET.
THEREFORE, THE LIKELIHOOD THAT
PEOPLE WILL REUSE PASSWORDS IS
GREATER.
ALSO PROBABILITY THAT THEY WILL USE SOMETHING REALLY SIMPLE IS GREATER.
THERE ARE LOTS OF RISKS HERE.
THE QUESTION I WANT TO START BY ASKING IS WHY IS IT THAT PEOPLE HAVE SUCH A HARD TIME WITH PASSWORDS ON PHONES WHEN THEY CAN KIND OF MANAGE IT ON DESKTOPS WHEN IN CONTRAST THEY'RE MANAGING SMS AND E-MAILING FRIENDS FROM THE PHONES VERY WELL.
ONE OF THE BIG DIFFERENCES IS THAT THERE'S AUTO CORRECTION.
ON SMS AND E-MAILS, IF YOU TYPE THE WRONG WORD THE RIGHT WORD APPEARS, THAT IS NOT THE CASE OF COURSE FOR PASSWORDS BECAUSE WE DON'T ENABLE AUTO CORRECTION FOR PASSWORDS.
SECOND QUESTION TO ASK IS, WHY ARE GOOD PASSWORDS HARD TO RECALL.
THIS IS NOT IN THE CONTEXT ONLY EVER MOBILE BUT IN GENERAL.
AND THAT'S BECAUSE WE WANT -- WE AS A COMMUNITY WANT PASSWORDS TO BE WEIRD.
WE WANT THEM TO BE UNPREDICTABLE, HAVE A SPECIAL CHARACTER AND COUPLE OF NUMERALS AND THIS IS NOT HOW HUMANS RELATE TO THINGS.
I MEAN WE'RE DESIGNING PASSWORDS AS CREDENTIALS THAT SHOULD BE MEMORIZED BY HUMANS NOT MACHINES.
IT'S ABSURD TO ASK PEOPLE FOR ALL THESE SPECIAL THINGS THAT PROBABLY AREN'T GOING TO BE THAT RANDOM AFTER ALL.
IF YOU LOOK AT THE DISTRIBUTION OF THINGS IF YOU ASK PEOPLE TO PUT SOME DIGITS AFTER THE WORD THAT THEY PUT, SOMETHING LIKE
1976, WHICH IS YEAR THAT YOU MIGHT HAVE BEEN WORN, OR SOMEBODY YOU KNOW HAS BEEN BORN IS MUCH MORE COMMON THAN NUMBER SUCH AS 1742. A YEAR YOU OBVIOUSLY WERE NOT BORN. SO THERE IS A VERY UNEVEN DISTRIBUTION. THE PEOPLE WHO MANAGE THE CORPORATIONS, LOG-IN CENTERS THEY DON'T KNOW BECAUSE THEY DON'T SEE THE PASSWORDS THEY DON'T ACTUALLY TOUCH PASSWORDS THEY STORE THEM IN A SAFEWAY BUT THE ATTACKERS DO. THE ATTACKERS SEE THE PASSWORDS THEY KNOW WHAT WE DON'T KNOW UNLESS WE TAKE UNUSUAL MEASURES. SO, NOW ME SHOW YOU A STAB AT A SOLUTION TO ADDRESS BOTH OF THESE THINGS AT THE SAME TIME. IMAGINE ALLOWED TO USE A WORD AS A PASSWORD THAT IS NOT A GOOD PRACTICE BECAUSE, WELL, FIRST OF ALL THERE AREN'T THAT MANY WORDS. BUT ONE NICE ASPECT SAY THAT YOUR PASSWORD NOW IS "FROG" YOU FAT FINGER AND RIGHT "FROTH." NOT A WORD. BUT THE APPLICATION, GOOD PASSWORD ENTRY WOULD KNOW THAT G-N-F ARE CLOSE AND FROF IS NOT A WORD BUT IT WOULD AUTOCORRECT. THAT TAKES CARE OF ONE BIG PROBLEM HERE. WHICH IS THAT IT'S CONSTRAINED INPUT. NOW, THE PROBLEM OF COURSE IS THAT THEY'RE ABOUT 64,000 WORDS NOT ALL WORDS ARE EQUALLY COMMON. YOU'D FIND "LOVE" MUCH MORE COMMON THAN HOMOMORPHIC. THIS IS ANOTHER PROBLEM WITH IT,
OF COURSE. IF YOU TAKE THREE WORDS AFTER EACH OTHER, YOU ACTUALLY GET VERY GOOD SECURITY AND IT'S STILL ALLOWS FOR AUTOCORRECT. SO THAT IS SOMETHING THAT IN MY VIEW IS BETTER TO DEAL WITH THAN PASSWORDS. IT'S SIMPLER ON A HAND SET. LET ME SHOW YOU SOME GRAPHS FOR SPEED. THIS IS THE GREEN LINE HERE IS THE TIME IT TAKES, THIS IS CUMULATIVE DISTRIBUTION HOW LONG IT TAKES TO ENTER SIMPLE PASSWORD. THE RED ONE IS A STRONG PASSWORD THE BLUE LINE HERE WHAT I'VE SHOWN YOU WHICH I JUST CALL A FAST WORD. THE PORTION OF USERS ON THE X AXIS, IT MEANS IF YOU LOOK AT THE RADIO%, IT'S HALF WAY ALONG X AXIS. YOU'D SEE THAT ALMOST ALL OF THE SIMPLE AND STRONG PASSWORDS CLOSE TO 100% FALL IN THAT -- THEY THAT I 100 SECONDS OR ABOUT TO ENTER. WHERE AS 50% OF THE FAST WORDS TAKE ONLY ABOUT FIVE TO TEN SECONDS TO ENTER. THIS IS A HUGE DIFFERENCE IN TERMS OF THE TIME IT TAKES, BECAUSE AUTO CORRECTION AND AUTO COMPLETION WORKS IN OUR FAVOR. NOW IF YOU LOOK AT THE SECURITY, THIS MIGHT NOT MAKE SENSE UNLESS YOU UNDERSTAND SECOND LOGARITHMS THIS IS A GUESSING PROBABILITY IN LOG 2, THIS IS THE AVERAGE FAST WORD SECURITY WHERE AS HERE OFF THE SCALE IS THE AVERAGE PASSWORD ABOUT 19 BITS OF SECURITY WHERE YOU HAVE MORE THAN 40 BITS OF SECURITY.
THIS IS BASED ON ACTUAL DISTRIBUTIONS.
ONE OTHER THING IN FAVOR OF THIS IS THAT YOU GOT DRAMATICALLY HIGHER RECALL RATES BECAUSE THREE WORDS THAT MEAN SOMETHING YOU CAN RELATE TO A STORY AS OPPOSED TO SOME NUMBER AND SOME STRANGE CHARACTER THAT YOU HAVE TO INCLUDE.
THAT'S A BENEFIT.
IF PEOPLE DO FORGET, IF THEY'RE FORCED TO USE DIFFERENT CREDENTIALS THEY CAN'T REMEMBER WHAT CREDENTIAL THEY USE IN ONE PLACE.
YOU CAN GIVE THEM A HINT, THE FIRST WORD SAY, YOU GOT TO REMEMBER THE OTHER TWO.
OF COURSE YOU DEGRADE THE BIT SECURITY BY ONE-THIRD BUT STILL IT'S MORE SECURE THAN A PASSWORD.
THE BENEFIT IS THAT NOBODY FORGETS.
SAY THAT YOUR STORY IS A WEIRD STORY WHEN YOU WENT JOGGING IN THE FOREST YOU STEPPED ON A SQL SERVER.
JOGGING FOREST SQL SERVER.
MAYBE YOU DON'T REMEMBER THAT THIS IS THE ONE YOU JUICE FOR LOG IN AT THE FINANCIAL INSTITUTION.
MOMENT YOU TOLD JOGGING YOU KNOW WHAT IT'S ABOUT.
LET ME TALK ABOUT SOMETHING COMPLETELY DIFFERENT.
HOW DO YOU AUTHENTICATE ON PLATFORM THAT DOESN'T HAVE A KEYBOARD NOT JUST A SMALL KEYBOARD BUT NO KEYBOARD AT ALL.
I'M GOING TO USE GOOGLE GLASS AS AN EXAMPLE.
APART FROM CAMERA AND MICROPHONE ALSO VOICE FEEDBACK, IT'S GOT A
TOUCH SENSOR THAT ALLOWS YOU TO SAY BACK, FORWARD AND UP. THOSE ARE THE THREE THINGS THAT BY RUBBING YOUR GLASSES YOU CAN COMMUNICATE. I'M GOING TO SHOW YOU HOW YOU CAN INPUT CREDENTIAL USING ONLY THAT. HERE THE CONTEXT IS VERY LIMITED OUTPUT. YOU HAVE TEENY TINY SCREEN. AND YOU GOT ADVERSARY THAT IN ESSENCE KNOWS EVERYTHING SHOW TO THE PUBLIC. IF YOU SPEAK OUT YOUR CREDENTIAL OR IF YOU MAKE GESTURES LIKE A "2" IN THE ERROR SHOW NUMBER THE ADVERSARY KNOWS ABOUT IT. THAT IS AN UNUSUAL SETTING THAT YOU COULD THINK OF HAND SET AS BEING AN INPUT OPPORTUNITY WHERE THERES NOBODY EAVESDROPPING. YOU CAN INPUT ON YOUR KNOWN WITHOUT SOMEBODY SEEING IT. BUT ON GOOGLE GLASS YOU CANNOT. CHANGE THE PIN TO YOURS. THAT'S ALL THE INSTRUCTION YOU'RE GIVEN. ASSUME THAT YOU ARE TYPICAL USER. THAT MEANS YOUR PIN IS 1, 2, 3, 4, SORRY TO SAY. STARTS AT RANDOM POINT THIS IS NOT YOUR PIN. YOU CAN SEE THERE'S A CURSOR YOU CAN SCROLL THAT UP AN DOWN ON GOOGLE GLASS CORRESPONDS TO FORWARD AND BACKWARD. IF YOU DON'T LIKE HAVING A 1 AS A FIRST CHARACTER THEN YOU CHANGE. THIS IS FORWARD THIS IS BACKWARDS. IF YOU LIKE 1 WHICH IN THIS CASE YOU DO. YOU ARE TAPPING SAYING NEXT.
TAP, YOU LIKE 1.
NOW YOU WANT A 2 HERE.
YOU GO BACK.
YOU GOT A 2.
YOU LIKE THIS.
YOU TAP.
5 IS NOT.
YOU GOT TO CHANGE IT.
NOW YOU CHANGE IT TO A 4.
THEN YOU SUBMIT.
NOW THE QUESTION IS, WHAT DID THE ADVERSARY LEARN?
NOTHING.
YOU STARTED RANDOM POINT,
ADVERSARY WHO KNOWS EVERYTHING
YOU'RE DOING FROM OBSERVING YOU,
MICROPHONES AND CAMERA, SEES YOU
RUBBING YOUR GLASSES.
NOT A BIG CLUE.
BUT YOU LOGGED IN.
THIS IS TO SAY THAT WHEN YOU
HAVE A NEW INPUT, OUTPUT
OPPORTUNITY THERE ARE DIFFERENT
ATTACKS BUT ALSO DIFFERENT
OPPORTUNITIES.
WE SHOULD TAKE ADVANTAGE OF
THEM.
THERE ARE LOTS OF THINGS THAT I
WOULD LIKE TO SPEAK ABOUT WHICH
I DON'T HAVE THE TIME TO SPEAK
ABOUT.
BUT WHICH I ENCOURAGE YOU IF
TAKE A LOOK AT.
IF YOU ARE INTERESTED HOW TO
AVOID SPOOFING, THERE'S A LINK
TO AN EFFORT THAT I'VE BEEN
INVOLVED IN.
HOW TO CREATE PINS IF YOUR USERS
DON'T HAVE ANY BUT HAVE
PASSWORD.
AND WHAT I TALKED ABOUT FIRST
BUT MORE DETAILS.
THANK YOU.
>> BEFORE WE GET IN TO THE
OTHER TWO PRESENTATIONS ABOUT
YOU A THEN OCCASION TECHNOLOGIES
I WANT TO PLAY THIS ONE CLIP FOR YOU.

§§

>> IT HAS BEEN REPORTED THAT IN THE FUTURE SIMPLY TYPING IN YOUR PASS CODE MAY BE OBSOLETE. HERE AT THE SCHOOL OF INFORMATION, RESEARCHERS ARE STUDYING THE USE OF BRAIN WAVE AUTHENTICATION AS AN ALTERNATIVE TO LOG INK TO COMPUTERS.

>> THERE IS LAPTOPS THEY CAN SCAN YOUR FINGERPRINTS, SECURE SYSTEMS THAT WOULD SCAN, FOR EXAMPLE, RETINA.

WE WANTED TO BUILD A SYSTEM WHERE WE WOULD SCAN SOMEONE'S BRAIN WAVES THEN WE WOULD USING THEIR BRAIN WAVES BE ABLE TO IDENTIFY THEM AND AUTHENTICATE THEM.

>> UNDERGRADUATE HAS BEEN WORKING WITH PROFESSOR AND HIS TEAM IN RESEARCH USE OF PASS DOTS.

HERE USERS THINK OF CERTAIN THOUGHTS OR IMAGES IN ORDER TO GAIN ACCESS TO THEIR COMPUTER DEVICES.

THE TEAM HAS BEEN USING THE COMPANY NEUROSKIES MINDSET DEVICE A BLUETOOTH HEADSET WITH A SENSOR THAT MEASURES THE DOMINANT BRAIN WAVES.

THIS SENSOR IS PLACED ON THE LEFT FRONTAL LOBE WHERE EMOTIONS AND MENTAL CONCENTRATIONS ARE MOST DOMINANT.

>> THE STUDY EXPERIMENTED WITH PARTICIPANTS TO PERFORMED MULTIPLE MENTAL TASK INCLUDING THINKING OF A REPETITIVE MOTION AND SINGING THEIR FAVORITE SONG. IN DOING SO HEADSET RECORDED AND MEASURED EACH INDIVIDUAL'S BRAIN
WAVES.
>> BRAIN WAVES ARE SIMILAR TO
         FINGERPRINTS ARE MEASURED
         THROUGH ELECTRO-- EEG SIGNALS.
>> EVERYONE HAS BRAIN WAVES.
         THAT ARE UNIQUE TO THEM.
         THIS COULD POSSIBLY BE A MORE
         UNIVERSAL FORM OF BIOMETRIC
         AUTHENTICATION.
>> THERE ARE SOME CONCERNS.
         THE TEAM HAS YET TO FIGURE OUT
         HOW TO STOP HACKERS.
>> IF AN ATTACKER KNEW THE
         USER'S PASS THOUGHT COULD THEY
         THINK THE SAME THING AND ABLE TO
         DUPE THE SYSTEM.
         THAT'S NOT SOMETHING THAT
         WE'VE -- THAT'S NOT REALLY
         SOMETHING THAT WE'VE HAD TIME TO
         LOOK IN TO BUT THAT WOULD BE
         POSSIBLE SECURITY CONCERN.
>> THAT'S JUST FOOD FOR THOUGHT
         FOR A MOMENT.
         NOW WE'RE GOING TO GET IN TO, WE
         HAVE TWO COMPANIES HERE WHO HAVE
         DEVELOPED AUTHENTICATION
         TECHNOLOGIES.
         ONE IS PASSBAN, THE OTHER IS
         YUBICO.
         KAYVAN DO YOU WANT TO TELL US
         ABOUT YOUR AUTHENTICATION
         TECHNOLOGY.
>> GREAT SECTION, LEARNED A
         LOT.
         TALK ABOUT THE DEATH OF A
         PASSWORD.
         I DON'T KNOW WHO IS GOING TO BE
         UNHAPPY ABOUT THIS.
         BUT SESSIONS I'VE SEEN SO FAR
         ALSO THE CONVERSATION
         SURROUNDING SECURITY, THE
         SELECTION OF A STRONG PASSWORD
         SOMETHING THAT'S COMPLEX AND
         CHANGING IT, I DON'T THINK
         PEOPLE LOOK FORWARD TO PUTTING
         UPPER CASE UNDERSCORE QUESTION
MARK UNDER SMALL PHONES TO LOG IN TO THEIR APPLICATIONS, NOT IN PUBLIC ENVIRONMENTS AND TRANSIT OR AT WORK.
THAT'S THE BAD NEWS.
GOOD NEWS IS THAT OVER THE PAST I WOULD SAY FOUR OR FIVE YEARS THE SMARTPHONES AND TABLETS THAT WE'VE GROWN ACCUSTOMED TO USING HAVE NOW BECOME EXTREMELY MORE POWERFUL IN THAT THE DEVICES ARE CAPABLE OF DETECTING WHO WE ARE BY OUR FACIAL RECOGNITION, WHAT WE SAY BY VOICE DETECTION, HOW WE MOVE A DEVICE THROUGH A GESTURE, OUR LOCATION.
WHAT WE WEAR AS A WEARABLE DEVICE AND PAIR WITH IT A SMARTPHONE OR TABLET. ULTIMATELY MORE ADVANCED METHODS SUCH AS PASS PHRASE THAT WAS JUST MENTIONED.
SENTENCES OR THE USE OF PASS COLORS, COLOR PALLET SHOWS UP YOU SELECT COLORS AS MEANS OF DETECTING OR IDENTIFYING YOURSELF.
ULTIMATELY THE IDEA BEING THAT THE DEVICES INCREDIBLY CAPABLE OF ACTUALLY PERFORMING EVERYTHING I JUST SAID WITHOUT THE NEED OF ANY ADDITIONAL EFFORT ON USER'S BEHALF.
YOU ARE WHO YOU SAY YOU ARE BECAUSE OF YOUR FACE, YOUR VOICE OR BECAUSE OF YOUR LOCATION OR SOMETHING THAT YOU'RE WEARING AS A RESULT FEED FOR REMEMBERING THE THAT CAN EASILY COMPROMISED AS I'M SURE A LOT OF YOU READ THE SAME ARTICLES AND PUBLICATIONS.
'THROUGOUT THREE HACKERS COMPETING ON HOW FAST THEY COULD DECRYPT 20,000 PASSWORDS.
STOLEN FROM A SET, COMPLETELY
ENCRYPTED WITHIN LESS THAN A DAY
ONE OF THEM WAS ABLE USING VERY
AVERAGE MODEST MACHINE DECRYPT
ALL THOSE PASSWORDS.
THIS IS FOREGONE CONCLUSION IN
OUR OPINION OBVIOUSLY THE
COMPROMISES WE'RE SEEING LEFT
AND RIGHT SOMETHING THAT SERVED
THEIR PURPOSE FOR LONG PERIOD OF
TIME BUT NOW WITH THE
CAPABILITIES OF THE DEVICES
WE'RE OF THE OPINION THAT
THERE'S MORE MODERN, MORE
SEAMLESS, FRANKLY MORE
CONVENIENT WAYS TO IDENTIFY USER
RATHER THAN ASKING THEM TO PUT
IN 16-DIGIT PASSWORD TO TAKES A
YEAR.
>> THAT'S REALLY THE IDEA TO
PROVIDE MOBILE SECURITY AND
INHERENT SOLUTIONS ON THE
SMARTPHONES AND TABLETS
CONSIDERING THE CAPABILITIES
THAT THESE DEVICES HAVE.
NOT GOING TO REPEAT THE
STATISTICS, OBVIOUSLY OUR STATS
ARE MORE AROUND GROUP OF -- SET
OF SURVEYS THAT WE DID AROUND
2,000 PEOPLE NOT NEARLY AS
ELABORATE AS THE REPORT WE HEARD
FROM CONSUMER REPORTS.
BUT BASICALLY FRUSTRATION OR I
DON'T WANT TO ENTER THIS DATA
WHAT THAT ENDS UP HAPPENING WITH
ALL OF THIS IS PEOPLE PUSH THAT
REMEMBER ME BUTTON, RIGHT?
YOU END UP NOT ENTERING THE
PASSWORD.
YOU USE, I DON'T KNOW THE
AUDIENCE HERE HOW MANY ENTERS A
PASSWORD TO GET IN TO YOUR
E-MAIL OR CALENDAR OR YOUR --
ANY APPLICATION YOU ARE
TYPICALLY LOOKING FOR THAT
"REMEMBER ME" MORE "KEEP ME
LOGGED IN" THAT'S NOT BECAUSE OF
THE LACK OF INTEREST IN SECURITY.
BUT MORE BECAUSE THEY WANTED TO PROVIDE THAT USER CONVENIENCE, ABILITY NOT HAVE TO ENTER THAT COMPLICATED DATA ON THE SYSTEM ON THE DEVICE.
THE CHALLENGES THAT WE SEE WITH SOME OF THE SOLUTIONS THAT -- SOME OF THE MORE SECURITY HALL THANKS PEOPLE FACE IS NOW YOU END UP SAYING, OKAY, I'VE INSTALLED 15 APPLICATIONS OR 20 APPLICATIONS ON MY SMARTPHONE IF I'M WANTING TO DO REAL TRUE MOBILE SECURITY THE RIGHT WAY I HAVE TO HAVE DIFFERENT PASSWORDS FOR EACH OF THESE APPLICATIONS. YOU END UP NOW HAVING TO MANAGE A GROUP OF PASSWORDS.
YOU ADD A QUESTION MARK, UNDERSCORE TO THE END OF THE OTHER.
IT BECOMES INCONVENIENT AND LEAKY AND EASY TO GUESS.
END UP USING SAME PASSWORD ACROSS MULTIPLE APPLICATIONS NOW JUST ONE SYSTEM NEEDS TO BE COMPROMISED FOR ALL OF YOUR DATA TO BE AVAILABLE.
ACTUAL PHONE SECURITY.
LOCK THE PHONE.
UNLOCK THE PHONE.
NOW EVERYTHING IS AVAILABLE TO THE END USER.
THIS MAY BE A GREAT SOLUTION FOR ACTUAL FIRST LINE OF DEFENSE, BUT IF YOU THINK OF A SHARED ENVIRONMENT OR ACTUAL COMPROMISES ARE HAPPENING WHERE DATA IDENTITY THEFT AND BASICALLY COMPROMISES OCCUR A LOT OF IT IS BY PEOPLE YOU KNOW, IS ACTUALLY AT HOME OR AT WORK WITHIN THE ENVIRONMENT.
ACTUALLY WORKING OR LIVE SO LOT
OF THESE DEVICES ARE ACTUALLY IN A SHARED ENVIRONMENT.
AT HOME FOR EXAMPLE WE HAVE IPAD THAT IS SHARED AMONGST FOUR PEOPLE.
AND THE PASSWORD IS 0000 BECAUSE MY 4-YEAR-OLD HAS TO BE ABLE TO USE IT AND I HAVE TO BE ABLE TO USE IT SHE CAN'T ENTER ANY OTHER DATA AS A PASSWORD YET.
IN A SHARED ENVIRONMENT LIKE THAT IF THE LOCKING FACTOR WAS MY FACE OR ANY OTHER WEARABLE DEVICE IN THE ABSENCE OF ME BEING THERE NOW NONE OF THE OTHER FAMILY MEMBERS USE THAT DEVICE SO MAYBE THE SOLUTION TO SAY, UNLOCK THE DEVICE AND USING VERY SIMPLE OR COMPLICATED PASSWORD TAKE YOUR PICK.
BUT SECURE THE APPLICATIONS AND CERTAIN TRANSACTIONS OR EVENTS THAT HAPPEN MAYBE ANGRY BIRDS DOESN'T REQUIRE PROTECTION OR ENCRYPTION OR PASSWORD-BASED ACCESS, MAYBE IT DOES YOU WANT TO PROTECT YOUR SCORE.
BUT MAYBE YOUR FINANCIAL OR BANKING APP OR HEALTH CARE APP THAT PROVIDES CRITICAL OR SENSITIVE INFORMATION ABOUT IS WORTH SECURING.
MAYBE DROPBOX DOESN'T NEED TO BE SECURED BUT SPECIFIC FOLDER AND PROVIDE AUTHENTICATION OR VERIFICATION THAT WOULD SOLVE THE PROBLEM.
THEN WE REALLY THINK THAT IT'S TIME FOR A LOT OF THESE PRODUCTS TO COME TOGETHER, YOU ARE HAVING IN TODAY'S PANELS YOU SEE SECURITY SOLUTION FROM APPLE AND USERS I'D FEE THEN GOOGLE HAS THE GOOGLE AUTHENTICATOR SOLUTION AND MICROSOFT HAS SIMILAR SOLUTION THEN COMPOUND
THAT, MULTIPLY BY A THOUSAND EACH HAS THEIR OWN WAY OF IDENTIFYING USERS.
IF YOU NOW START INTRODUCING MULTI-FACTOR OR FACE OR OTHER, YOU HAVE TO ENROLL IN TO EACH OF THOSE APPLICATIONS NOW SEPARATELY.
ACTUALLY CREATE BIGGER MESS THAN WE HAVE.
WE THINK THE TIME HAS COME FOR SINGLE IDENTITY, USING ONE FORM OF IDENTIFICATION ACROSS MULTIPLE APPLICATIONS.
THERE'S A LOT OF INITIATIVES SUCH AS FIDO STARTED TO ADDRESS THAT TOY MEANS OF BRINGING SOLUTIONS TOGETHER.
APPLICATION USAGES EXPLODING THAT'S OUR 10.4 BILLION DOWNLOADS DURING ONE QUARTER.
IS AMAZING THAT YOU THINK OF ANDROID AND PHONES THAT ARE COMMERCIALY USING THEM HOW LONG HAS IT BEEN TAKING US TO GET HERE TALK ABOUT FOUR OR FIVE YEAR TIME SPAN NOW TALKING ABOUT THIS NUMBER OF APPLICATIONS BEING DOWNLOADED.
IT'S A HEALTHY AND GROWING USAGE BY USERS, HOWEVER WE THINK THAT AS A RESULT OF SO MANY APPLICATIONS BEING DOWNLOADED ON DEVICES THAT ARE SO CAPABLE OF MULTI-FACTOR VERIFICATION CAPABILITIES IT'S TIME TO INTRODUCE THEM IN TO THESE APPLICATIONS.
SOME SURVEYS, WHAT APPS WOULD YOU SECURE, WHAT TRANSACTIONS WOULD YOU SECURE?
IT WAS INTERESTING TO ME THAT MYSELF I DON'T SECURE MY E-MAIL ON MY SMARTPHONE, JUST ACCESS GMAIL.
BUT IT WAS NUMBER TWO, IF PEOPLE
HAD CONVENIENT WAY OF SECURING E-MAIL BY SIMPLY USING A FACE OR A GESTURE OR MAYBE A WEARABLE, TAPPING ON WRISTBAND TO UNLOCK THE APPLICATION THEY WOULD USE IT.

ALSO SHOCKING PERSONALLY TO ME WAS THE NEED FOR REQUEST BY PEOPLE AGES 29 AND UNDER, 40% WERE ASKING, I WOULD PROTECT MY TWITTER OR FACEBOOK OR APPS THEY DON'T WANT OTHER PEOPLE TO SEE THE MESSAGES OR STREAM OF EVENTS HAPPENING ON THEIR PARTICULAR FACEBOOK PAGE.

ULTIMATELY WHAT WE'RE SEEING IS LOOKING FOR SOLUTIONS THAT ARE ADAPTIVE.

ONE THING ALSO THAT I WANT TO MENTION SOLUTIONS THAT END UP ASKING THE USER TO BE IN A PERFECT ENVIRONMENT FOR IT TO WORK.

FACE ONLY WORKS IF IT'S WELL LIT AND IF YOU'RE IN FRONT OF A GOOD CAMERA HAS THE RIGHT FRAME PER SECONDS.

USERS ARE NOT ALWAYS IN THOSE ENVIRONMENTS.

THERE HAS TO BE A METHOD OF ADAPTING TO THE USER'S ENVIRONMENT.

FLEXIBLE DEVICES, I HAD iPHONE NOW I'M ON ANDROID, NOW I'M USING iPAD.

THESE TYPES OF IDENTITY SOLUTIONS HAVE TO WORK ACROSS THESE DEVICES.

YOU DON'T WANT TO PUT THE USER THROUGH THE PROCESS OF REENROLLING AND REINTRODUCING MULTIPLE PASSWORDS THAT'S NOW A POSSIBILITY.

AND PLAY WELL WITH OTHERS.

SYSTEMS THAT ARE PROVIDING -- I CAN DO PASSWORD I CAN TOO FACE
BUT THIS DEVICE IS CAPABLE OF DOING VOICE VERIFICATION.
BRING THAT IN TO THE SOLUTION.
PLAY WELL WITH OTHERS THIS IS
ALSO NOW VERY MUCH A POSSIBILITY
TO USE THE CAPABILITIES OF THE
DEVICE BY INTRODUCE NEW METHODS
OF VERIFICATION.
ULTIMATELY PORTABILITY IN THAT
IF YOU ARE USING A DEVICE YOU,
LOSE IT OR GET STOLE THEN YOU
SHOULD BE Able TO USE THAT SAME
IDENTITY ON NEW DEVICE.
THESE ARE THE KIND OF I WOULD
SAY FOUR OR FIVE ITEMS THAT
WE'VE IDENTIFIED ASCII.
THANK YOU SO MUCH.
GO THROUGH THIS TO THE NEXT?
>> GREAT.
BEFORE WE GET IN TO QUESTIONS
ABOUT YOUR TECHNOLOGY, TERRY,
WOULD YOU LIKE TO TALK ABOUT
YUBICO'S NEW AUTHENTICATION
TECHNOLOGY.
>> I SURE WOULD.
THANK YOU VERY MUCH.
IT'S A PLEASURE TO BE HERE.
MY NAME IS TERRY SHOFNER THE
COMPANY IS YUBICO.
I'M GOING TO -- LISTENING TO
SOME OF THE CONVERSATIONS TODAY
TOOK ME BACK SAID I'M NOT A
SCIENTIST, I'M NOT A
TECHNOLOGIST, I AM AN ENGINEER
THAT WENT TO SCHOOL, WHEN I
GRADUATED I SAID, MAN, I GOT A
JOB.
I POLLED A LOT OF PEOPLE WAS
ABLE TO KEEP GOING WITH THIS
THING.
WHAT I'M GOING TO TRY TO DO
BRING IT TO A LEVEL WHEN THIS
WAS PROBABLY A CORN FIELD THINK
ABOUT THE GUYS DOWN THE HILL
THAT HAD THEIR MAJOR ASSET WAS
THEIR HOME.
I'M GOING TO TAKE THAT JUST
CARRY THAT WITH ME, STAY WITH ME
A LITTLE BIT.
I KNOW IT'S GETTING LATE IN THE
DAY, YOU HAD A HOME, YOU
PROBABLY DIDN'T LOCK IT.
YOU PROBABLY DIDN'T HAVE KEYS.
BUT EVENTUALLY PEOPLE STARTED
USING KEYS TO LOCK THE DOORS ON
THEIR HOME.
THEN ABOUT A HUNDRED YEARS AGO
SOMEBODY CAME UP WITH AN
AUTOMOBILE.
THAT WAS A COOL DEVICE, TOO, IT
WAS ALSO A MAJOR ASSET.
THIS MAJOR ASSET IN THOSE DAYS,
THAT DIDN'T HAVE KEYS.
THE TRICK THERE WAS JUST, DO YOU
KNOW HOW TO DRIVE IT.
A FEW PEOPLE DID, SO THAT WAS
THE -- HOW YOU WERE PROTECTED.
BUT EVENTUALLY KEYS CAME IN TO
PLAY.
TODAY YOU HAVE KEYS THAT ARE
QUITE SOPHISTICATED.
YOU WALK UP, YOU GET CLOSE, IT
OPENS UP, THERE IS SOME
TECHNOLOGY THAT MAKES THAT FUN
AND MAKES IT EASY TO USE.
THEN NOW TODAY WE LIVE IN A
WORLD WHERE OUR ASSETS ARE TIED
UP IN BANK ACCOUNTS OR WE'RE
WORKING ON THE INTERNET.
THINK -- I KNOW EVERYONE KNOWS
HOW IMPORTANT IT IS TO HAVE
ACCESS TO THE INTERNET.
YOU CAN LOSE YOUR PHONE, YOU CAN
BE WITHOUT A PHONE OR BE WITHOUT
A HOME PHONE BUT TAKE AWAY
INTERNET ACCESS FOR A DAY YOU
GOT PROBLEMS OR AT LEAST I DO.
BECAUSE I CAN'T DO MY JOB.
THERE'S SO MANY THINGS THAT I
CAN'T DO.
THE CELL PHONES TODAY BECOME
SMARTPHONES AND IT KEEPS GETTING
BETTER AND BETTER.
BUT THERE IS STILL ONE COMMON
THING TO THAT, YOU HAVE A KEY.
THAT'S WHERE I'M GOING TO SHARE
WITH YOU A LITTLE BIT.
ASSUME THAT I JUST HIT AN ARROW
AND WE GO FORWARD.
IF YOU GO BACK 20 YEARS AGO,
technology came up, we started
thinking and talking about two
factor authentication.
what you have, what you know.
this has been around for a long
time basically in very
competitive modes but very
similar.
this product works the same way.
where i'm going back is a little
bit on legacy user names and
passwords are broken, some of
the statistics that we've
borrowed from you are a trillion
in one year that's a lot of
hacking.
now going in to malware and bad
things that are happening but
i'm just talking about things
that can happen and get in to
your phone or your data, used to
be your house, used to be your
car.
now it's getting in to the cloud
and services that you're using
on a daily basis.
if you look at smartphones and
it goes to one of my associates
about how difficult it is to
take a smartphone, if you're
going to use user name or pin
then plug in, not a four but
maybe six, maybe 12 character
that's pretty tough stuff to do.
especially when you're as clumsy
as i am it's very difficult to
do.
The awkward of doing a product
THAT IS LEGACY DRIVEN THERE ARE SOME THINGS THAT ARE OUT THERE THAT ARE COMING ALONG THAT ARE BETTER.

THE COMPANY YUBICO HAS BEEN AROUND FOR ABOUT SEVEN YEARS, THE EARLY DAYS IT WAS A VISION THAT SOMEONE HAD OF TAKING A TOKEN, USB TOKEN, INSERT IN TO A PC, AGNOSTIC TO THE OPERATING SYSTEM WHETHER IT'S A MAC OR PC YOU CAN JUST TOUCH THIS BUTTON, TOUCH THAT BUTTON YOU WOULD GENERATE 44 CHARACTER, ONE TIME, AES ENCRYPTED PASSWORD, THAT'S COOL.

WHEN YOU DID IT, YOU DIDN'T HAVE TO REPEAT IT. YOU DIDN'T MAKE A MISTAKE BECAUSE IN THIS CASE IT'S EVENT DRIVEN, IF YOU SCREW IT UP LOST YOUR CONNECTION YOU GO BACK TOUCH THE BUTTON AGAIN.

THE PRODUCT THAT WE'RE TALKING ABOUT IS THIS LITTLE THING. WATERPROOF TO 50 METERS, NO BATTERIES, NO LCD, NOTHING. JUST INSERT IT TOUCH THE BUTTON AND GO.

THIS IS WHERE WE GOT OUR FOOTING.
WE HAVE BEEN GROWING, WE CONTINUE TO GROW, TODAY WE'RE SPEAKING IN TERMS OF MILLIONS. IF I KNEW HOW TO DO THIS. I KNOW WHAT I'M DOING. WE WERE LIMITED TO THE USB DEVICE. THAT'S STILL GOOD. BECAUSE WE HAVE A LOT OF PEOPLE THAT HAVE BEEN SITTING ON THESE PANEL, IS THAT ARE USING THEIR PRODUCT IN THE ENVIRONMENT. IT'S A USB DEVICE.

THE IDEA, THE NAME YUBICO COMES FROM-FOUNDER SAID, THE IDEA ARE
YOU TO BE UBIQUITOUS.
THERE'S A MESSAGE HERE THAT I'M
GOING TO, HAVING A SINGLE TOKEN
THAT'S READILY AVAILABLE, THAT
YOU CAN USE AS A CONSUMER.
MAKE CONNECTION SECURELY TO
WHERE YOU NEED TO WORK OR WHERE
YOU NEED TO GO, IS A PRETTY GOOD
AND POWERFUL THING.
WHAT HAS HAPPENED, THE
TECHNOLOGY, PEOPLE IN OUR
COMPANY, SMARTPHONES, CONSUMERS,
WE ALL PRETTY MUCH ALL OF US
WILL HAVE ONE OF THESE PHONES.
THIS ONE JUST HAPPENS TO BE AN
ANDROID.
I'M GOING TO THINK ABOUT WHAT
YOU DO TODAY, TO AUTHENTICATE IF
YOU DON'T USE PASSWORDS THAT'S
PROBABLY NOT A GOOD THING BUT IF
YOU DO IT'S GOOD.
I'M JUST TURNED ON THIS PHONE.
I PUT IN MY PASS PHRASE.
NOW -- HERE IS MY YUBIKEY.
I'M TOUCHING THIS TO THE BACK OF
THE PHONE.
WHAT JUST HAPPENED I OPENED THE
BROWSER, ENTERED THE URL, SENT A
44 CHARACTER ONE TIME PASS CODE
AND LET ME GET IN.
NOW, I DIDN'T HAVE TO REMEMBER
ANYTHING, IT WASN'T MY FACE, IT
WASN'T MY BREATH, IT WASN'T MY
D.N.A.
IT WAS SIMPLY TOUCHING SOMETHING
THAT I HAVE THAT IS A SECURE
ELEMENT, I MIGHT ADD, CONNECTED
UP TO MY SERVER FOR ME TO DO MY
WORK.
ONLY DIFFERENCE IS, I DID THIS
FOR WOW PURPOSES.
I DIDN'T PUT MY PIN NUMBER IN.
I USE THE SWIPE CODE.
BUT THIS IS WHERE WE THINK THE
WORLD IS GOING.
AFFORDABLE, FAST.
THINK ABOUT NO SUPPORT.
THINK ABOUT YOUR SUPPORT ISSUES
PRETTY MUCH GOING AWAY.
THIS THING GETS EVEN BETTER.
BECAUSE CAN YOU IMAGINE A TOKEN
LIKE THIS THAT HAS AN APPLET ON
IT OR COULD BE -- COULD HAVE
MONEY STORED ON IT WHEN YOU TO
GO YOUR STARBUCKS YOU TOUCH IT
TO THE TOKEN AND WALK AWAY.
IT'S CIV READY.
ANYWAY, THEN GOING ON TO SOME OF
THE CONVERSATIONS ON THE
STANDARDS.
IT'S BEEN SORT OF WILD WEST FOR
AWHILE.
THERE SEEMS TO BE NOW AN
EMERGING GROUP OF PEOPLE PUTTING
THEIR HEADS TOGETHER SAYING,
OKAY, WHAT'S THE BEST PROTOCOL.
WE'RE PART OF THAT GROUP.
WE PARTNERED WITH GOOGLE AND
ANOTHER MANUFACTURER CALLED NXP
THAT IS IN CHIP MANUFACTURING
WORLD.
ONE OF THE CONCEPTS WE THINK IS
GOOD WAY TO APPROACH THE MARKET.
SORT OF THE END OF THE DAY YOU
HAVE THIS STANDARD, UNIVERSAL
FACTOR, YOU'RE A USER YOU HAVE
YOUR YUBI KEY OR USING YOUR
PHONE OR PC OR TABLET.
ANYTHING IN THIS CASE I DIDN'T
QUALIFY THAT IT HAS TO BE NFC
READY.
WHICH IS PRETTY MUCH EVERYBODY
OUT THERE EXCEPT FOR ONE
MANUFACTURER.
BUT THESE DEVICES ARE READY.
YOU CAN GO TO YOUR RETAIL STORE
YOU CONNECT THEN YOU CAN DO YOUR
BANKING OR YOU CONNECT TO THE
SERVICES THAT ARE OUT THERE.
JUST ENVISION WHAT THIS IS READY
TODAY.
THIS IS A PRODUCT, THIS IS NOT
THE FUTURE WHAT WE'RE OFFERING
OUT FOR YOU TODAY.
YOU HAVE ABILITY TO DO SINGLE
SIGN, ALL THESE THINGS, PASSWORD
MANAGERS COMPANY OUT CALLED LAST
PASS, IF YOU HAVE A YUBI KEY IT
INTEGRATES WITH THEM.
WE'RE HOPING SEE THE BANKING
TAKE A HOLE RECOGNIZE THIS AS
GOOD WAY TO GO.
THAT'S IT.
THANK YOU VERY MUCH.
>> THANK YOU, TERRY.
I THINK MARKUS WOULD LIKE TO
COMMENT.
>> JUST WANT TO BRIEFLY MENTION
THAT ON THE TOPIC OF PASSWORD
MANAGERS OF COURSE THIS IS WHERE
IT TIES IN TO THE WHOLE MALWARE
DISCUSSION BECAUSE THAT'S ONE
STOP SHOPPING OPPORTUNITY FOR
THE MALWARE AUTHORS TO STEAL ALL
THE CREDENTIALS AT THE SAME
TIME.
THIS IS GOOD TOUCH POINT BETWEEN
THE TWO PORTIONS.
TO RECOGNIZE THIS IS WHERE IT
MATTERS.
>> BEFORE WE GET IN TO THAT.
I WANT TO JUST TALK ABOUT ONE
THING THAT KAY VON SAID ABOUT
KEEPING YOUR DEVICE UNLOCKED.
THE PURPOSE OF I GUESS USING MY
OWE METRICS IN YOUR
AUTHENTICATION THAT YOU ONLY
HAVE TO AUTHENTICATE -- YOU
WOULD LOCK INDIVIDUAL APPS
WOULDN'T LOCK YOUR PHONE IT
WOULDN'T LOCK YOUR APPS.
>> OR BOTH.
THE IDEA WAS TO BE ABLE TO USE
THAT SAME DEVICE IN SHARED
ENVIRONMENT.
IF THERE IS ONE PASSWORD, SO
IDEA WAS LOWER THE BAR MAYBE FOR
LOCKING DEVICE BUT INCREASE BAR
FOR SELECTIVE APPLICATIONS THAT
NEED TO BE SECURE.
>> I'D LIKE TO -- BOTH KAYVAN
AND TERRY, YOUR AUTHENTICATION
TECHNOLOGIES HOW WOULD THOSE
HELP CONSUMERS WHO HAVE ACTUALLY
HAD THEIR PHONES STOLEN.
WE'RE TALKING ABOUT
AUTHENTICATING GET ON TO APPS OR
WEBSITES BUT IF SOMEONE'S PHONE
IS LOST OR STOLEN HOW WOULD
THAT -- SEEKS THAT YOUR PHONE
WOULDN'T NECESSARILY BE LOCKED
ITSELF, RIGHT?
DEVICE ITSELF NECESSARILY BE
LOCKED.
YOUR APPS OR YOUR --
AUTHENTICATING YOURSELF ON A
WEBSITE.
>> TYPICALLY WHEN YOUR PHONE IS
LOST YOU'RE PROBABLY LESSEE MOCK
PHYSICALLY ATTACHED TO THE PHONE
_THAN THE DATA THAT YOU LOST ON
THAT PHONE.
THAT DATA IS AGAIN IF YOU THINK
OF THE STATISTICS, WHAT APPS YOU
ARE RUNNING ON THAT PHONE
PROBABLY TWO OR THREE OR FOUR OF
THOSE APPS MAYBE PICTURES,
MESSAGES AND SOME APPLICATION
THAT IS STORING MOBILE CONTENT
LOCALLY THAT YOU'RE VERY, VERY
INTERESTED IN NOT PROVIDING
UNAUTHORIZED ACCESS.
A LOT OF GREAT ACCESS PROVIDE
REMOTE WIPING.
NOW THAT YOU FOUND OUT IT'S LOST
AND STOLEN AS LONG AS DEVICE IS
NOT TAKEN OFF THE NETWORK YOU
CAN PROVIDE REMOTE WIPE
CAPABILITIES.
THE APPLICATION THAT THE
SOLUTION THAT WE'RE ADVOCATING
WOULD THEN SAY, IT'S FINE.
THE DEVICE IS LOST OR STOLEN
IT'S USELESS IN THE WRONG HANDS
BECAUSE THAT PERSON WHO STOLE THE DEVICE HAS TO ALSO BE YOU FROM BIOMETRICS PERSPECTIVE OR WEAR YOUR WEARABLE DEVICE OR FACTOR THAT TERRY WAS JUST EXPLAINING.
IT SIGNIFICANTLY INCREASES THE BAR IN TERMS -- RAISES THE BAR IN TERMS OF PREVENTING ANNOTATE RISED ACCESS.
>> LET ME BUILD ON THAT JUST A LITTLE BIT MORE.
IT'S THE SAME THING, THE DIFFERENCE IF YOU LOSE THE PHONE BUT IN OUR CASE YOU HAVE TO HAVE THE TOKEN AND YOU HAVE TO HAVE THE PIN NUMBER SO IT'S WHAT YOU HAVE AND WHAT YOU KNOW.
YOU STILL HAVE TO HAVE THAT TO ACCESS THOSE APPLICATIONS.
IN OUR WORLD WE'RE TAKING A STANDARD YUBIKEY USE IT ACROSS THE BOARD WITH MANY APPLICATIONS.
ON THE BACK END THE COMPANIES THAT SUBSCRIBE -- THAT'S NOT THE RIGHT WORD.
THAT THAT USE THE AUTHENTICATION MECHANISM THAT WE PROVIDE THEY'RE GOOD TO GO.
THOSE MAY BE DIFFERENT.
IT'S NOT THE SAME.
BECAUSE IT CHANGES EVERY TIME YOU TOUCH THAT BUTTON.
BUT YOU ARE GENERATING THAT ONE TIME PASSWORD OR THE SECURE ELEMENTS GENERATING THE WAY THAT IT LINKS SO THAT IT DOESN'T MATTER.
YOU CAN'T GET IN TO THOSE APPLICATIONS.
>> MARKUS I THINK YOU WERE STARTING TO TOUCH ON THEN THE SECURITY VULNERABILITIES I GUESS OF THESE AUTHENTICATION TECHNOLOGIES IS THAT SOMETHING
THAT YOU COULD EXPAND ON.

ONCE YOU SPEAK ABOUT USER AUTHENTICATION, OF COURSE, THE MOST PRACTICAL PARADIGM IS TO AUTHENTICATE TO YOUR DEVICE THAT YOUR DEVICE AUTHENTICATE TO THE WEBSITE.

THAT MEANS THAT YOU HAVE STORAGE OF CREDENTIALS.

THEY THAT HAVE PIECE THAT ARE STORED ON THE DEVICE.

IT MIGHT BE THAT THEY'RE SANDBOXED DEPENDING ON IMPLEMENTATION.

MIGHT BE THAT THE CODE IS HARD INNED.

BUT NEVERTHELESS THE CREDENTIALS ARE ON THE DEVICE.

THIS IS WHERE AUTHENTICATION MEETS MALWARE.

BECAUSE THAT IS THE SOURCE OF MONETIZATION FOR THE MALWARE.

EXACTLY THAT STORAGE.

SO DO YOU SEE THIS AS NOT A BENEFIT THEN FOR CONSUMERS?

THIS IS WHY MANY LARGE FINANCIAL INSTITUTIONS DO NOT SUPPORT PASSWORD MANAGERS, THAT'S ALL I'M SAYING.

IT'S A COST RISK BENEFIT.

IF ANYBODY IN THIS ROOM WANTS TO USE PASSWORD MANAGER THAT'S PROBABLY SAFE BUT IF THE SOCIETY AS SUCH SWITCHES TO PASSWORD MANAGER OF ANY KIND IT'S GOING TO CAUSE A NEW TYPE OF FRAUD IN WHICH YOU WON'T SEE PHISHING BUT MORE MALWARE.

LET ME JUST SAY ALSO THAT THESE PASSWORDS ARE ALREADY STORED ON THESE DEVICES.

WHENEVER YOU PUSH THAT "REMEMBER ME" BUTTON BY DEFAULT ASKING FOR THAT INFORMATION TO BE CASHED OR STORED.

TO MARKUS' POINT TALKING TO
VARIETY OF DIFFERENT PEOPLE WE GET I DON'T WANT BY BIOMETRIC DATA TO BE STORED TO ANY OF MY BIOMETRIC DATA TO BE STORED. EACH OF THEM HAVE THEIR GOOD REASONS FOR IT. SOME OF THEM TO YOUR POINT ABOUT THE DEVICES MOST VULNERABLE IN THE WRONG HANDS THAT CAN HACK IN TO IT, DECRYPT IT AND ACCESS IT. ALSO IF YOU ARE STORING INFORMATION ON THE SERVER NOT PROVIDING THAT LOCAL CACHE DATA YOUR ASKING FOR TRANSMISSION OF DATA.

>> I NEED TO CLARIFY, TOO, BECAUSE WE'RE NOT IN OUR CASE THE PASSWORDS ARE NOT STORED, THAT PHONE THAT I JUST USED DEMONSTRATION I TOOK OUT OF THE BOX YUBIKEY I TURNED ON THE NFC CAPABILITY I TOUCH IT. IT GOES TO MY SERVER. THERE'S NO PASSWORD, THERE'S NO APPLICATION. THIS IS WORKING DIRECTLY OFF OF THE FIRM WEAR THAT'S INSIDE OF THE KEY. I MAY NOT HAVE -- SOMETHING ELSE THAT WE WORK WITH TO BE MANY, MANY THOUSANDS OF THINGS. MORE PEOPLE IN THE CONSUMER WORLD ARE TRYING USE THINGS THAT THEY GET AWAY FROM SO MANY PASSWORDS THAT HAVE TO CHANGE. IT'S SORT OF EASY WAY OUT. I'M CERTAINLY NOT PROMOTING THAT I'M JUST SAYING THAT SOMETHING WE WORK OUT OF THE BOX WITH.

>> YOU WANT TO SAY SOMETHING?

>> ONE DIFFERENCE BETWEEN SAVING YOUR PASSWORDS LIKE CHECKING THE BOX "REMEMBER ME" AND USING PASSWORD MANAGERS LIKE THE POPULAR OR -- WHEN YOU USE THOSE MANY USERS DON'T KNOW
THEIR PASSWORDS ANY MORE THEY
AUTO GENERATE RANDOM PASSWORDS
WHICH THEY HAVE NEVER EVEN SEEN
THEMSELVES.
WHEN YOU SAVE YOUR OWN PASSWORD
YOU KNOW A PASSWORD THIS OPENS
UP A NEW ANGLE OF ATTACK WHICH
IS RANDOM 'TOX NOT TO STEAL
CREDENTIALS.
BUT TO TAKE AWAY THE CREDENTIALS
FROM THE USERS AND MAKE THE USER
PAY TO REGAIN ACCESS TO SYSTEMS
WHERE HE HAS NO PASSWORDS ANY
MORE HE NEVER KNEW THEM.
WE'VE SEEN RANDOM MALWARE RAISED
IN POPULARITY.
WE HAVEN'T SEEN ATTACKS LIKE
THIS BEFORE.
>> CHANGING GEARS SLIGHTLY ON
THIS.
I THINK SOMEONE MENTIONED THAT
THE MAJORITY OF MOBILE USERS
DON'T HAVE PASSWORDS ENABLED ON
THEIR DEVICES.
ONE THING THAT I WAS REALLY
STRUCK BY ON GOOGLE GLASS WAY TO
IN PUT A PASSWORD I WAS JUST
THINKING LIKE, WOW, COULD YOU
THINK OF WORSE WAY TO
AUTHENTICATE ON A WEARABLE
DEVICE.
WE HAVE TO THINK ABOUT, TALK
ABOUT THE FUNDAMENTAL PROBLEM
HERE WHICH IS FACT THAT USERS
DON'T -- MAJORITY OF USERS -- IN
SORT OF USABLE WAY.
AS WE MOVE FORWARD FROM JUST --
YOU HAVE LOT MORE OPTIONS THAN
JUST A PIN CODE.
WHEN YOU TALK ABOUT MULTI-FACTOR
AUTHENTICATION, PAIRING
SOMETHING YOU KNOW WITH
SOMETHING YOU HAVE WE CAN EXPAND
THE WORLD OF THINGS THAT WE
KNOW, SIGNIFICANTLY.
BEYOND JUST ENTERING A PIN.
GLASS, FOR INSTANCE, HAS GAZE DETECTION YOU CAN ACTUALLY -- ACTUALLY WINK THAT COULD BE VIEWED AS INPUT. I WAS FORTUNATELY BLESSED BY GOOGLE TO HAVE THE CHANCE TO PAY THEM $1500 TO USE GLASS. THERE IS ACTUALLY AN OPEN SOURCE DEVELOPED OUT THERE THAT VERY SIMILAR TO WHAT MARKUS MENTIONED. IT'S CALLED BULLETPROOF. THAT LET'S YOU ENTER PASSWORD BECAUSE BASICALLY GLASS DOESN'T COME WITH A PIN CODE FOR SECURITY PURPOSES. IT'S SIMILAR TO WHAT MARKUS MENTIONED BUT INSTEAD OF SELECTING DIGITS IT INTERPRETS SWIPES AS UNIQUE IDENTIFIERS. YOUR PASS TOWARD TO LOG IN TO BE SWIPE FORWARD TWICE, TAP, TAP. WHEN WE TALK ABOUT SOME OF THESE NEW OPTIONS TOWARDS AUTHENTICATION AND MULTI-FACTOR, I THINK IT'S USEFUL TO REMEMBER THAT I THINK RUMORS OF THE DEMISE OF THE PASSWORD ARE GREATLY EXAGGERATED. I THINK THAT THERE'S ALWAYS GOING TO BE ROOM FOR ONE PIECE OF AUTHENTICATION WHICH IS SOMETHING THAT YOU KNOW. NOW WE JUST HAVE TO NOT BE MYOPIC ABOUT WHAT IS MEANT BY THAT. >> I THINK IS THE MESSAGE TO CONSUMERS THEN THAT -- IN LIGHT OF THE STATISTICS OF LOST AND STOLEN PHONES AND CONSUMERS WHO DON'T USE PASSWORDS AT ALL. SO THEIR DATA IS MUCH MORE AT RISK. WHAT IS THE MESSAGE TO CONSUMERS TO CONTINUE TO USE PASSWORDS THAT ARE HE'SLY CRACKED, THAT
They reuse them.
They lose them.
Or is it to move nor war in one of these new authentication type of technologies, biometrics, what is the message to consumers who don't even want to use a password to begin with?
>> I'm not in the position to solve the problem, these guys are solving it. Whatever the solution is it's got to be something that most ordinary people are willing to do.
We're all kind of geeky, I know I am, and maybe willing to tap-tap, twigs-twigs or blink-blink, not many people in my family are.
I don't think people doing that don't want to punch four digits slide their finger to open a phone.
I don't see them getting in to mother's code with their eyes and fingers.
You also have to think about non-technical people who they're willing to actually do.
>> I wouldn't want to in still hope that they're going to go 'weigh way entirely.
After all when you get a new device you need to kind of introduce yourself to that device.
That's one form of authentication.
And the other one before it can learn your biometrics or download them for example, another kind to recovery.
So if somehow you cannot use biometrics or somehow your Yubico device was lost or you
PUT IT, YOU DON'T KNOW WHERE IT IS, SOMEBODY TOOK IT FROM YOU, I DON'T KNOW WHAT WOULD HAPPEN. YOU NEED A BACK UP. THE INTERESTING THING IF YOU USE A PASSWORD EVERY DAY YOU PROBABLY REMEMBER IT. IF YOU USE IT TWICE A WEEK, YOU PROBABLY DO, TOO. BUT IF YOU USE IT TWICE A YEAR YOU'RE NOT. SO, WE ARE MOVING IN A DIRECTION WHERE IT'S MORE CONVENIENT TO THE USER BECAUSE OF BIOMETRICS BUT WHEN DISASTER HAPPENS IT'S REALLY BAD. YOU NEED FOB ABLE TO ENTER A CREDENTIAL THEN AND YOU SHOULD NOT HAVE FORGOTTEN IT. THAT'S THAN INTERESTING DILEMMA. >> I WOULD ALSO SAY THAT IT'S IMPORTANT THAT WE DON'T ENCOURAGE CONSUMERS TO GET A FALSE SENSE OF SECURITY WITH SOME OF THESE NEW TECHNOLOGIES THAT ARE EMERGING. THERE IS STILL DEPENDENT ON THINGS LIKE PASSWORDS ESPECIALLY IN THE SHORT TERM. AND ENFORCING JUST REASONABLE BEHAVIOR IN TERMS OF REASONABLE COMPLEXITIES AS WELL AS BEING GENERALLY PARANOID. GENERALLY A GOOD THING. EVEN RIGHT NOW SORT OF ALL DEPENDS ON YOUR THREAT MODEL BUT I THINK ALMOST EVERYONE IN THIS ROOM RIGHT NOW KNOWS TERRY'S PASSWORD ON HIS PHONE. FROM HIS PRESENTATION, I COULD UNLOCK HIS PHONE RIGHT NOW IF I HAD A LEAD PIPE. IT SORT OF DEPENDS ON YOUR MODEL. >> I'D LIKE TO MOVE IN TO THE NEXT AREA NOW WE'RE GOING TO
TALK ABOUT ANTI-THEFT AND ANTI-VIRUS TECHNOLOGIES THAT ARE SOLUTIONS FOR CONSUMERS. THIS IS I THINK PARTICULARLY RELEVANT BECAUSE, FIRST OF ALL JEFF HAS SAID THAT IN THE CONSUMER REPORT STUDY THAT TWO OF THE MAIN RISKS TO CONSUMERS ARE LOST OR STOLEN PHONES AND MALWARE.

WE LEARN THIS MORNING THAT THERE IS A BIG MALWARE PROBLEM, THERE ISN'T A BIG MALWARE PROBLEM FOR U.S. CONSUMERS. WE WILL GO IN TO THOSE STATISTICS RIGHT NOW.

WE KNOW THAT I JUST TO THROW OUT SOME STATISTICS ABOUT STOLEN PHONES. CONSUMER REPORTS FOUND THAT 1.6 MILLION SMARTPHONES WERE STOLEN LAST YEAR.

AND THERE WAS RECENT LOOK HOT SURVEY THAT FOUND ONE IN TEN PEOPLE IN THE U.S. HAS THEIR PHONES STOLEN.

IN NEW YORK CITY 11,000 APPLE DEVICES WERE REPORTED STOLEN IN A NINE-MONTH PERIOD.

IN DC 40% OF THE ROBBERIES IN 2012 INVOLVED CELL PHONES. GIVEN THAT BACKDROP I LIKE DEREK AND MIKKO TO GIVE THEIR PRESENTATIONS.

>> OKAY.

FIRST I'LL TRY TO KEEP THIS QUICK SO WE'RE ON TIME. BUT LOOK HOW WE BUILD TOOLS TO HELP PEOPLE USE THEIR MOBILE DEVICES WITH CONFIDENCE. SINCE AROUND 2007, WE PROVIDED A SET OF FEATURES ORIENTED AROUND SECURITY THAT INCLUDE THING LIKE DATA BACK UP, ANTI-MALWARE PROTECTION. PROTECTION FOR LOST AND STOLEN
DEVICES.
ABILITY TO REMOTELY LOCK AND WIPE DEVICES.
SINCE THAT TIME IT'S BECOME FEATURE SET THAT'S SOMEWHAT RECOGNIZABLE.
THE FACT OF STANDARD FOR SECURITY ON SORT OF THE MOBILE PLATFORM.
WE'VE HEARD A LOT ABOUT DURING TODAY'S DISCUSSIONS ABOUT SORT OF RELATIVE DEGREES OF RISK THAT PEOPLE ARE FACED WITH.
WE HAVE BEEN IN UNIQUE POSITION TO HAVE BEEN TRACKING A NUMBER OF THESE THREATS FOR A NUMBER OF YEARS.
I WANTED TO PROVIDE A LITTLE BIT OF CONTEXT ACROSS A FEW THINGS THAT HAVE BEEN MENTIONED TODAY.
WE HAVE SEEN THAT IN 2012 ESTIMATED 1.4 MILLION U.S. ANDROID USERS ENCOUNTERED A BAD APP OVER THE COURSE OF 2012. THAT'S A MILLION PEOPLE THAT'S A LOT OF PEOPLE.
BUT WHEN YOU TALK ABOUT PERCENTAGES THAT EQUATES TO PRETTY SMALL CHANCE OF ACTUAL ENCOUNTERING MALWARE IN THE U.S. JUST HOVER 1%.
SMARTPHONE PENETRATION IS PRETTY IMPRESSIVE IN THE U.S. IF YOU LOOK CLOSER THAT RATE VARIES TREMENDOUSLY NOT GEOGRAPHICALLY.
I KNOW THAT WE'RE FOCUSED ON REALLY U.S. PROBLEMS IN THIS CONTEXT, JUMPS TO AROUND 40% IN RUSSIA AROUND 20% IN CHINA.
WHERE WE'RE REALLY BROAD BASED ECONOMICALLY DRIVEN ATTACKS HAVE LOT MORE FREEDOM TO OPERATE FOR I THINK A NUMBER OF REASONS THAT HAVE BEEN DISCUSSED AT LENGTH.
COMPARE THAT TO THE FACT THAT
AROUND FOUR IN TEN PEOPLE CLICKED ON AN UNSAFE LINK FROM THEIR MOBILE DEVICE IN 2012. WHAT DO I MEAN. A PHISHING LINK, COMPROMISED WEBSITE, SOMETHING THAT MIGHT TRIGGER A DRIVE BY DOWNLOAD WITHOUT THEIR KNOWLEDGE. STATISTICALLY SPEAKING MUCH MORE PREVALENT PROBLEM AND EQUALLY TROUBLING ONE PARTICULARLY BECAUSE OF THE RESTRICTIONS THAT WE'VE TALKED ABOUT IN TERMS OF WHAT MOBILE PRESENTS FROM A FORM FACTOR.

TO SCROLL PAST NOT REALLY SEE WHAT YOU ARE URL FACT THAT COLLEEN MENTIONED IT NEARLY 10% OF THE PEOPLE IN THE U.S. HAVE HAD A PHONE STOLEN. WE FOUND THAT ACTUALLY THROUGH SURVEY EARLY THIS YEAR. WHEN YOU FACTOR IN THE ECONOMICS HERE THIS ONE BECOMES MUCH BIGGER THAN THE OTHERS REALLY A DRIVING FACTOR.

WE ESTIMATE THAT IT COST CONSUMERS AROUND $30 BILLION IN 2012. WHICH IS NO LAUGHING MATTER. I'LL BE HAPPY TO DEEP MORE DETAIL ON THE FIRST AND SECOND ITEMS ON THIS LIST BUT I WANTED TO SORT OF DIVE IN TO THIRD ONE WHICH IS NOT QUITE AS COMMONLY DISCUSSED WITHIN THIS CONTEXT. THAT'S ONLY ONE COMPONENT OF IT.

WHAT WE FOUND WAS THAT THEFT IS MUCH MORE THAN -- REPRESENTS MUCH MORE THAN PHYSICAL LOSS. WHEN ASKED -- WE ASKED CONSUMERS OUT THERE WHAT THEY WERE CONCERNED ABOUT SURE THE MONETARY DOWNSIDE WAS ONE THING, BUT LOSS OF DATA WAS REALLY SORT OF COMPOUNDING FACTOR, IF YOU
WILL.
AND SO THINKING HOW WE'RE
ACTUALLY SOLVING THIS PROBLEM.
NOT TALKING ABOUT MALWARE FOR
THE TIME BEING HOW WE SOLVE THIS
PROBLEM.
I'M REMINDED BY A QUOTE FROM ONE
OF OUR INVESTORS THAT I THINK, I
MAY BE UP WITHERING HERE NO
CELLARER BULLETS ONLY LEAD ONES.
YOU CAN STACK A BUNCH OF
DIFFERENT SOLUTIONS TOGETHER
POTENTIALLY TO HELP SOLVE THIS
BUT REALLY IT'S SIMILAR TO
DISCUSSION ON PREVIOUS PANEL
AROUND PATCHING.
YOU CAN'T JUST SNAP YOUR FINGERS
AND TALL OF A SUDDEN IT'S
SOLVED.
WHAT ARE SOME OF THE THINGS WE
CAN THINK ABOUT.
NUMBER ONE, EDUCATION
EMPOWERMENT IS BIG.
PEOPLE OFTEN TALK ABOUT
EDUCATION PIECE OF IT.
RAISE AWARENESS, BASICALLY TELL
PEOPLE THEY CAN PUT PASSWORDS ON
THEIR PHONE.
THAT'S GREAT.
BUT IT'S NOT VERY USABLE AND NOT
VERY EFFECTIVE IF THE TOOLS YOU
GIVE TO THEM AREN'T REALLY
DRIVING THEM TO USE THEM.
IF ONLY THE MAJORITY OF USERS
OUT THERE AREN'T PUTTING
PASSWORDS ON THEIR PHONES THEY
PROBABLY HAD SOMEONE SCOLD THEM,
WHETHER IT'S THEIR TEENAGE SON
OR DAUGHTER OR WHETHER THEY HAVE
COWORKER WHO IS NOTICED IT.
BUT THERE'S OBVIOUSLY SOMETHING
WRONG WITH THE PROCESS PEOPLE
ARE STILL SORT OF NOT ADOPTING
WHAT SHOULD BE SORT OF BASIC
FUNDAMENTAL TENAMENT.
SOME OF THE THINGS THAT WE TRY
TO DO, LOOKOUT ARE TO IMPROVE
SOME OF THE BASIC FEATURES.
MAKE THEM MORE ENGAGING AND MORE
USABLE.
ONE REALLY SIMPLE EXAMPLE WAS A
TOOL, FEATURE CALLED SIGNAL
FLARE WHICH HELPS YOU FIND A
LOST OR STOLEN PHONE THAT MAYBE
RUNNING LOW ON BATTERY ENDS YOU
AN E-MAIL WITH A DEVICE’S
LOCATION ON A MAP.
AS THE PHONE IS RUNNING OUT OF
BATTERIES YOU CAN ACTUALLY FIND
IT IF IT'S -- IF IT HAS RUN OUT
OF BATTERY.
SECOND ONE CALLED, LOCK CAM
IDENTIFY ANYONE WHO TRIED TO LOG
IN TO YOUR PHONE, PRESUMING YOU
HAVE A PASSWORD, OF COURSE.
THREE TIMES INCORRECTLY YOU CAN
SEE THAT MAYBE ON THIS PHONE OUR
PANEL MODERATOR HAS BEEN BUSY
WHILE I'VE BEEN AWAY FROM MY
PHONE.
SECOND ONE IS MARRYING
TECHNOLOGY WITH LAW ENFORCEMENT.
WE'VE BEEN REALLY BUSY WITH THE
DISTRICT ATTORNEY’S OFFICE IN
SAN FRANCISCO AND A.G. IN
NEW YORK AROUND ENABLING LAW
ENFORCEMENT TO WORK EFFECTIVELY
WITH TECHNOLOGY COMPANIES WHEN
IT COMES TO SOLVING THIS LOST
AND STOLEN DEVICE PROBLEM.
THE THIRD IS REALLY INCENTIVE,
'O, RIGHT, NOT SO MUCH.
IT'S ACTUALLY TOUGH ONE TO SOLVE
HERE AND WE THINK ABOUT WHAT'S
DRIVING THIS PROBLEM AT LEAST
WHEN IT COMES TO STOLEN DEVICES
NOT JUST LOST ONES FACT THEY CAN
BE RESOLD OR REPURPOSED AT AN
ECONOMIC GAIN.
THERE IS A MUCH BROADER
COOPERATION NEEDED TO SOLVE THIS
PROBLEM.
BETWEEN OPERATORS, PLATFORM, OEMs, ET CETERA.
THE FCC MANDATED STOLEN DEVICE DATABASE IS A NICE STEP IN THE RIGHT DIRECTION.
WAY, WAY OVERDUE TO BE HONEST.
BY CONTRAST EUROPEAN OPERATORS ESTABLISHED THE EIR WHICH IS EQUIPMENT IDENTITY REGISTER TO HOLD A LIST OF HAND SET.
RECENT CALLS TO ENABLE SORT OF KILL SWITCH AS IT WERE ON MOBILE PLATFORMS AND OPERATORS THAT HAS VARIOUS PROS AND CONS.
>> THANK YOU.
MIKKO.
>> WHEN WE LOOK AT THE FLAT FORM SPLIT, WE'LL LOOK AT THE OPERATING SYSTEMS WE ARE RUNNING, IT'S BEEN THE CASE FOR THE LAST 20 YEARS MOST OF THE MICROSOFT PLATFORMS, WINDOWS HAS ALWAYS BEEN -- ESPECIALLY PROBLEMS MICROSOFT HAS BEEN FACING, HOWEVER, IF WE LOOK AT THE SITUATION RIGHT NOW IN 201 IN A LITTLE BIT MORE DETAIL WE'LL SEE THAT THE THREE MOST COMMON PLATFORMS YOU MIGHT BE RUNNING ON YOUR COMPUTER ARE THE SAME THREE MOST COMMON PLATFORMS YOU MIGHT BE RUNNING ON YOUR SMARTPHONE.
BECAUSE YOUR COMPUTER IS EITHER RUNNING WINDOWS OR OSX OR LINUX DISTRIBUTION.
YOUR PHONE IS EITHER RUNNING WINDOWS OR IOS OR SOME LINUX DISTRIBUTION.
THAT'S TOP THREE FOR BOTH.
OF COURSE WITHIN WE SPEAK ABOUT LINUX AND PHONES WE MOSTLY MEET ANDROID.
AS WE KNOW COMPUTER SIDE IT'S ALL WINDOWS PROBLEMS.
ALMOST ALL OF THE MALWARE WE
FIND STILL TODAY.
IN FACT MOSTLY A LITTLE BIT
OLDER WINDOWS ESPECIALLY WINDOWS
XP WHICH IS NOW 11 YEARS OLD
WHICH WILL BE OUT OF SUPPORT BY
MICROSOFT NEXT YEAR, YET IT IS
THE SECOND MOST OPERATING
SYSTEM, WINDOWS 7, XP NUMBER TWO
THEN WINDOWS VISTA.
IT WOULD BE EASY TO MAKE THE
MISTAKE OF -- WOULD HAVE BEEN
EASY TO GUESS COUPLE OF YEARS
AGO THAT IT'S GOING TO BE
EXACTLY THE SAME ON PHONES.
BUT AS WE NOW KNOW IT LOOKS
EXACTLY THE OPPOSITE.
ON PHONES WINDOWS PHONE HAS NO
MALWARE.
NO MALWARE.
LINUX, IN THIS CASE, ANDROID HAS
ALL MOBILE PHONE.
THERE'S MUCH LESS MOBILE PHONE
WEAR.
THAT'S PRETTY MUCH HOW IT WORKED
OUT.
APPLE ON BOTH SIDES HAS A LITTLE
BIT.
THIS IS QUITE SURPRISING.
IN FACT ANDROID BECAME THE FIRST
LINUX DISTRIBUTION THAT FINALLY
GOT THE MALWARE PROBLEM IN TO
THE LINUX WORLD.
IT WAS ANDROID THAT REALLY
BROUGHT THE PROBLEM THERE.
THERE'S BEEN SEVERAL MENTIONS
THROUGHOUT THE DAY ABOUT
DIFFERENT STATISTICS AND GROWTH
RATE -- I'M NOT GOING THROUGH
ANY DETAILS JUST MAKE A NOTE
THAT WE PUT OUT A MOBILE THREAT
REPORT WITH DETAIL STUDIES AND
FULL BLOWN NUMBERS ABOUT THE
GROWTH RATE OF THE PROBLEM.
WHEN WE SPEAK ABOUT MOBILE
MALWARE AND ANDROID MALWARE, THE
PROBLEM CAN PRETTY MUCH BE
DISTILLED IN TO THIS.
THIS HERE IS ANGRY BIRDS FROM
ROVIO DOWNLOADED FROM GOOGLE
PLAY.
THIS HERE IS ANGRY BIRDS FROM
ROBIO DOWNLOADED FROM GOOGLE
PLAY.
ONE OF THEM IS TROJANIZED.
ONE IS ORIGINAL, ONE IS A GAME,
ONE OF THEM IS A GAME AND DOES
SOMETHING BAD LIKE DIALS OUT TO
TOLL NUMBERS.
HOW DO YOU TELL THE DIFFERENCE,
YOU CAN'T.
HERE IS SCREEN SHOT FROM -- IT
HAS GRAND THEFT AUTO, SIMS,
HAYDAY IS MADE BY COMPANY CALLED
SUPER CELL.
HERE IT'S NOT MADE.
MY CRAFT IT'S ALL DONE BY
GILBERT.
GRAND THEFT AUTO AND S IRRMS IS
MADE BY EA, ELECTRONIC ARTS.
YES, GOOGLE DOES VERY GOOD JOB
IN LIMITING STUFF LIKE THIS,
GETTING IN TO GOOGLE YET THEY
SOMETIMES GET TO GOOGLE PLAY.
I JUST CHECKED THIS VERY SIMILAR
EXAMPLE LIKE THIS ON GOOGLE PLAY
RIGHT NOW, IF I WOULD HAVE LIVE
INTERNET CONNECTION I'D SHOW
YOU.
YES, GOOGLE KICKED THEM OUT VERY
QUICKLY WE HAVE TO BE FAST.
THEY DO EXIST.
YES WHEN WE TRY TO ILLUSTRATE
THE DIFFERENCE IN THE PROBLEM
SIZE ON YOUR COMPUTER AND YOUR
PHONE THE BEST EQUIVALENT I CAN
GIVE YOU THE DIFFERENCE BETWEEN
SIZE OF SON AND EARTH.
WE HAVE A MASSIVE PROBLEM WITH
PC MALWARE MOSTLY WITH WINDOWS
COMPUTERS.
YES WE HAVE PROBLEM WITH MOBILE
MALWARE, NO WHERE NEAR.
IN FACT YOU COULD SAY THAT MOBILE SECURITY IS A SECTIONIST STORY.
THAT'S A BIT -- OVER STATE BUT WE'RE CLOSE TO IT.
YEARS AGO, NINE YEARS AGO FOUND VERY FIRST MOBILE PHONE VIRUS,
CALLED KABIR IN SUMMER 2004.
IF I WOULD HAVE ESTIMATED THAT WHAT WOULD THE SITUATION LOOK LIKE TEN YEARS IN TO THE FUTURE I WOULD HAVE ESTIMATED MUCH MORE GRIMMER SITUATION.
I WOULD HAVE ESTIMATED WE'D HAVE MASSIVE WORM-LIKE SMS SPREADING MALWARE ALL MAJOR MALWARE AND PLATFORMS.
AND MILLIONS OF INFECTIONS.
THAT'S NOT WHERE WE ARE.
WE SEEM TO BE ABLE TO LEARN FROM PAST MISTAKES.
NONE OF THE PLAYERS IN MOBILE SPACE WANT TO REPEAT THE MISTAKES THAT WE'RE DONE WITH THE PC PLATFORM.
THE SITUATION CLEARLY IS MUCH BETTER.
WE MANUFACTURE JUST LIKE -- MOBILE SECURITY SOLUTIONS, WE HAVE LOTS OF OPERATOR CUSTOMERS, LOTS OF CONSUMER CUSTOMERS RECALL OVER THE WORLD.
HOWEVER VAST MAJORITY OF THOSE DON'T GET OUR MOBILE SECURITY PRODUCT TO FIGHT MALWARE.
BECAUSE THEY DON'T THINK MALWARE IS A PROBLEM.
THEY'RE CORRECT.
THE PROBLEM IS VERY LIMITED.
IT'S UNLIKELY, MUCH MORE LIKELY TO RUN IN TO PC MALWARE.
MOBILE SECURITY SOLUTIONS IS FOR OTHER BENEFITS LIKE THE REMOTE LOCATE, REMOTE LOCK, REMOTE WIPE.
OR WEB FILTER OR, FOR EXAMPLE,
WE HAVE FILTER FOR -- YOU CAN FILTER OUT TEXTS OR CALLS FROM CERTAIN NUMBERS IF YOU HAVE IRRITATING NEIGHBOR WHO KEEPS CALLING YOU -- HE CAN'T CALL YOU ANY MORE.
STUFF LIKE THAT.
OUR REMOTE LOCAL WIPE SYSTEM HAS BEEN DESIGNED TO WORKS WITH TEXT MESSAGES.
YOU DON'T NEED TO HAVE INTERNET CONNECTION YOU CAN JUST TEXT YOUR LOST PHONE FROM ANYBODY'S PHONE, MENTION THAT -- FOR EXAMPLE YOU CAN SEND TEXT SAYING, LOCATE.
IT WILL RESPOND BACK WITH A TEXT MESSAGE WHICH GIVES YOU GOOGLE MAPS LINK.
OF COURSE ONE THING WHICH HAS BEEN MENTIONED SEVERAL TIMES IS PHISHING AND OTHER WEBSITE CONTENT.
WEB FILTER FUNCTIONALITY YOU GIVE A TABLET OR A SMARTPHONE TO A CHILD YOU WANT TO MAKE SURE THAT SHE OR HE WON'T BE ABLE TO ACCESS WEBSITES ABOUT VIOLENCE OR DRUGS OR PORN, YOU WANT TO BE ABLE TO LIMIT THAT FUNCTIONALITY.
EVEN NORMAL USER WHO DON'T NEED WEB FILL YOU STILL WANT TO FILTER OUT PHISHING CONTENT.
LIKE HAS BEEN MENTIONED EARLIER IN THE PANEL OR PREVIOUS PANELS PHISHING IS A REAL PROBLEM.
THANK YOU.
>> JUST GO BACK TO SOMETHING YOU HAD SAID ABOUT COOPERATING WITH LAW ENFORCE: THE D.A. IN SAN FRANCISCO IS ACTUALLY BEEN VERY PUBLIC ABOUT CALLING FOR A TECHNOLOGICAL SOLUTION TO LOST -- STOLEN PHONES.
ASKING FOR A KILL SWITCH THAT
WOULD PERMANENTLY DISABLED THE PHONE UPON THEFT.
SO I WANT TO ASK YOU WHAT DO YOU THINK THAT HAVE IDEA OF A KILL SWITCH AND HOW WOULD THAT -- WITH THAT DEBT TRIMENTHOLLY AFFECT CONSUMERS DO YOU THINK?
>> IT HAS A NICE RING TO IT, DOESN'T IT.
KILL SWITCH.
TURN THAT PHONE OFF.
IT DEPENDS ON THE DEGREE TO WHICH IT'S IMPLEMENTED.
AS IT GOES WITH A LOT OF THESE POLARIZING TYPES OF QUESTIONS, THE ANSWER IS SOMEWHERE IN THE MIDDLE.
LIKE I MENTIONED DURING MY REMARKS I THINK IT'S BEEN WAY TOO LONG TO HAVE ANY SORT OF ANTI-THEFT SOLUTION IN PLACE WITHIN THE U.S.
EVEN THE SOLUTION THAT'S DEEMED BY FCC IT DOESN'T INTEGRATE DIRECTLY WITH THE EIR IN EUROPE. SO IT LEAVES OPEN POTENTIAL TO JUST SHIP HANDSETS THAT -- MIGHT BE COMPATIBLE WITH NETWORKS IN EUROPE THERE YOU GO.
I THINK THERE'S NUMBER OF DIFFERENT ISSUES AT HAND.
I THINK ONE POTENTIAL OTHER ISSUE THAT ARISES IS, LET'S SAY YOU DEVELOP A KILL SWITCH, THAT'S GREAT.
NOW WHO WATCHES THE WATCHERS, AS IT WERE.
The KILL SWITCH IS ALL OF A SUDDEN ONE NEW POTENTIAL VULNERABILITY THAT COULD BE TAKEN ADVANTAGE OF AND PRESENTS OWN SET OF SECURITY ISSUES.
I THINK THAT MOVEMENT IN THIS DIRECTION IS PROGRESS BECAUSE WHERE WE'RE AT RIGHT NOW THERE'S NOT NEARLY ENOUGH PROTECTING
USERS THAT'S I THINK OBVIOUS FROM JUST THE MASSIVE NUMBER OF LOST AND STOLEN DEVICES THAT ARE OCCURRING RIGHT NOW.
BUT WE HAVE TO BE CAREFUL ABOUT WALKING BEFORE WE RUN.
>> THIS REMINDS ME OF THE DISCUSSION REGARDING THE GREAT BIG INTERNET KILL SWITCH TO BE USED BY THE PRESIDENT OF THE UNITED STATES OF AMERICA.
MY COMMENT BACK THEN WAS THAT IF YOU BUILD A KILL SWITCH DON'T BE SURPRISED IF SOMEONE OPENS PRESSES IT.
>> ONE OTHER QUESTION ANTI-THEFT THEN JUST DO, ONLY HAVE TIME FOR MAYBE ONE OR TWO QUESTIONS ON ANTI-VIRUS IS THERE WAY FOR INDUSTRY TO SOLVE THIS PROBLEM?
I THINK THIS IS EQUATED TO THE PROBLEM WITH CAR THEFTS.
SO CAR THEFTS HAVE GONE DOWN SIGNIFICANTLY SINCE AUTOMOBILE MANUFACTURERS HAVE INSTITUTED ANTI-THEFT TECHNOLOGY IN TO CARS.
IS THERE A SIMILAR TECHNOLOGICAL SOLUTION DO YOU THINK FOR PHONES TO REDUCE THE INCENTIVE FOR THIEVES TO STEAL THOSE PHONES.
>> I DO THINK SO.
I THINK THERE'S AN OPTION AND ROOM FOR IMPROVEMENT HERE.
WHEN WE TALK ABOUT THE ECONOMIC DRIVERS HERE, IT'S ABOUT RESELLING THE DEVICE OR REALLY SHIPPING IT OFF SOMEWHERE TO BE RESOLD AS A USED OR REFURBISHED DEVICE.
WHEN YOU PUT ADDITIONAL BARRIERS IN PLACE THAT SORT OF DRIVE UP THE ECONOMIC COST FROM THE BAD ACTOR'S PERSPECTIVE YOU GENERALLY REDUCE INCENTIVE.
THAT SAID, THERE IS I THINK ALWAYS WILL PROBABLY BE WAYS TO SORT OF FIDDLE WITH DEVICE IDENTIFIER SO IF KILL SWITCHES ARE SORT OF PRIMARILY ACTING ON A NUMBER OF DEVICE IDENTIFIERS THAT ARE SORT OF HARDWARE BASED, THERE ARE ALWAYS COMPLEX WAYS TO GET THOSE TO CHANGE, IF YOU ARE DETERMINED ATTACKER BUT WHAT WE'RE TALKING ABOUT HERE IS TRYING TO HAVE AN AFFECT ON THE LOWEST -- ESSENTIALLY THE LOW HANGING FRUIT HERE. THAT IS OPPORTUNISTS AND REDUCING THEIR ABILITY TO REALLY SORT OF MAKE A QUICK BUCK ON THIS.

>> MARKUS YOUR COMPANY, FATSKUNK, OFFERS AN AV SOLUTION KNOWN AS SOFTWARE BASED. HOW DOES THAT DIFFER FROM THE PRODUCTS THAT HAVE LOOK OFFERS TO CONSUMERS.

>> IT ISN'T FOR CONSUMERS.
IT'S ACTUALLY TO BE BUILT IN TO THE INFRASTRUCTURE.

>> HOW DOES IT BENEFIT CONSUMERS LIKE THAT.

>> IT BENEFITS CONSUMERS BY HAVING NOT ONLY CONSUMERS, WHAT IT DOES IT ALIGNS THE ABILITIES TO DETECT WITH THE LIABILITY. THOSE WHO NEED TO DETECT AREN'T ALWAYS THE CONSUMERS. IT'S THE FINANCIAL SERVICE PROVIDERS AND SO ON THEY CAN DETERMINE IF YOU HAVE MALWARE. IF SO THEY CAN REDIRECT YOUR -- THE WAY IT DOES COMPUTER SCIENTISTS REFER AS EXTREME VERSION OF THE TIME SPACE TRADE OFF.

FOR THE NUMBER PERSON IT MEANS THAT YOU STOP ALL PROCESSES THEN YOU RUN SOMETHING VERY WOULD YOU
TAKESSAL INTENSIVE.
THAT TAKES MUCH LONGER IF THERE IS DEPRESSANT OF ANYTHING ON THE PHONE.
IF ANYTHING IT’S THERE ON THE PHONE AND EXECUTING WHICH -- THEN IT WILL TAKE LONGER TIME FOR YOUR PROCESS TO EXECUTE THERE FOR SOMEBODY OBSERVES THE TIME IT TAKES TO EXECUTE.
THAT SOMEBODY IS ALIGNED WITH WHOEVER CARES SO THAT YOUR BANK, FOR EXAMPLE, CAN TELL IF YOUR PHONE IS INFECTED.
YOU CAN ENCRYPT PORTIONS OF YOUR DEVICE BY HAVING SOMEBODY HOLD KEY TO THAT ONLY RELEASE IT WHEN THE -- THIS IS NOT SOMETHING THAT CONSUMERS WOULD PURCHASE.
MORE WHAT -- WHOEVER DEALS WITH THE CONSUMERS, ENTERPRISES AND FINANCIAL INSTITUTIONS, THAT SAID, IT IS NOT ON THE MARKET EITHER.
WE DO HAVE IT RUNNING ON ANDROID DEVICE BUT STILL 2349 CONCEPT STAGE.
>> IT WOULD BE ON THE BACK END.
CONSUMERS WOULD NEVER EVEN KNOW THAT IT WAS THERE.
>> DEVICES WILL SHIP WITH IT.
CONSUMERS OR FINANCIAL SERVICE PROVIDERS OR EMPLOYERS CAN ENABLE IT.
AFTER WHICH IT CAN BE SELECTIVELY ENABLED FOR CERTAIN RESOURCES YOU HAVE TO PERFORM -- IS NOT NOTICEABLE TO THE CONSUMER IS NOT RUNNING WHEN THE SPAN IS NOT INITIATED.
IT'S A DIFFERENT KIND OF PARADIGM IT DOESN'T BLOCK MALWARE TO GET FROM YOUR DEVICE BUT IT DOES BLOCK MALWARE FROM GETTING ABLE TO MONETIZE YOUR DEVICE.
YOU CAN'T GET ACCESS.
SO IT'S A GOOD COMPLEMENT TO
CODE HARDENING AND TRADITIONAL
ANTI-VIRUS APPROACH.
TO ANSWER YOUR QUESTION IT'S NOT
AN ALTERNATIVE.
BUT A COMPLEMENT.
>> THAT LEADS ME TO MY LAST
QUESTION I GUESS BECAUSE WE'RE
OUT OF TIME.
GIVEN THE STATISTICS THAT WE'VE
HEARD TODAY THAT IT SEEMS LIKE
MOBILE MALWARE ISN'T AS HUGE OF
A RISK FOR U.S. CONSUMERS RIGHT
NOW.
WHAT SHOULD THE MESSAGE BE TO
CONSUMERS ABOUT PUTTING
ANTI-VIRUS ON THEIR PHONES.
SHOULD THIS -- CONSUMERS BE
DOING THIS IS IT REALLY
NECESSARY OR NECESSARY BECAUSE
AS MIKXO SAID IN CONJUNCTION TO
HAVING THE ANTI-THEFT THAT
TECHNOLOGY AS WELL THAT THAT'S
REALLY BENEFICIAL TO CONSUMERS.
>> WE TALK A LOT ABOUT ONE END
OF THE SPECTRUM HERE IN TERMS OF
APPLICATIONS.
STUFF THAT'S GOING TO STEAL YOUR
MONEY AND EAT YOUR BABIES AND
THINGS LIKE THAT, IT'S -- THAT
END OF THINGS I THINK THAT THE
RISK LIKE WE'VE ALL COME TO
AGREE IS FAIRLY LOW.
I THINK THAT THERE'S A BROADER
OPPORTUNITY HERE THAT'S NOT
NECESSARILY BEING OPENLY
DISCUSSED THAT HAS TO DO WITH
THE REST OF THE CONTINUUM OF
APPLICATIONS.
THERE'S A LOT GOING ON ON YOUR
MOBILE DEVICE THAT THE MAJORITY
OF CONSUMERS DON'T REALLY HAVE A
FULL GRASP ON.
WHEN YOU TALK ABOUT MOVING
BEYOND THE SET OF APPLICATIONS
THAT ARE CLEARLY MALICIOUS TO THIS SORT OF VAST GREY AREA IN THE MIDDLE, WHERE SOME INFORMATION ABOUT YOU MIGHT BE COLLECT OR SOME INFORMATION ABOUT DEVICE MIGHT BE COLLECTED, THERE'S ALMOST SORT OF WILFUL IGNORANCE IN PLACE BECAUSE OF THE COMPLEXITY THAT BRINGS WITH IT.

AT LEAST FROM THE STANDPOINT OF LOOKOUT, WE LOOK AT MALWARE AND SPYWARE AND SURVEILLANCE WEAR AS JUST ONE PIECE IN EDUCATING CONSUMERS ABOUT THE RISKS OF THESE MOBILE DEVICES. WHAT WE WANT TO BE ABLE TO PROVIDE TO THEM IS REALLY AN OPPORTUNITY TO MAKE AN INFORMED CHOICE ABOUT WHAT'S GOING ON IN THEIR DEVICES.

WE THINK THAT AT LEAST RIGHT NOW THE FUNDAMENTAL PIECES IN PLACE FROM PLATFORM ARE ARE NOT GREAT. ANDROID YOU BREEZE BY PERMISSION SCREEN BECAUSE YOU REALLY WANT TO PLAY THAT GAME BUT YOU DON'T KNOW WHAT REPERCUSSION, IS THAT HAS IN TERMS OF BEING COLLECTED ABOUT YOU.

I THINK THE RECOMMENDATION TO CONSUMERS IS, IS BROADER. IF YOU ARE INTERESTED IN UNDERSTANDING, OF COURSE SOME PEOPLE MAYBE AREN'T, WHAT IMPLICATIONS YOUR MOBILE USE HAS THERE'S AN OPPORTUNITY TO SORT OF LEARN THAT AND MAKE MORE INFORMED CHOICES BY USING APP LIKE A SECURE.

>> WE'RE OUT OF TIME.
>> OUR ADVICE TO CONSUMERS DEPENDS ON YOUR EXPOSURE. WE'VE FOUND LOT OF PEOPLE ONLY HAVE TEN OR 20 APPS ON THEIR PHONE IF YOU DON'T DOWNLOAD A
LOT OF APPS YOU STICK WITH SOURCES LIKE GOOGLE PLAY AND THE iTUNES APP STORE YOU'RE RELATIVELY SAFE. IF YOU ARE VERY ACTIVE, DOING A LOT OF APPS YOU GOT A LOT OF SENSITIVE INFORMATION YOUR EXPOSURE IS GREATER IT WOULD BE PRUDENT THING TO USE ANTI-VIRUS. >> TEN SECONDS OR LESS. >> WE'D LOVE TO SEE ALL THE CONSUMERS IN TALL ANTI-VIRUS BEFORE THE FIRST GLOBAL HUGE MASSIVE OUTBREAK HAPPENS BUT REALISTICALLY, THEY PROBABLY WILL INSTALL IT ONLY AFTER IT. >> THANK YOU. [ Applause ] >> MY NAME IS CHUCK HARWOOD I'M HIJACKING THE CONFERENCE. I AM THE ACTING DIRECTOR FOR BUREAU OF CONSUMER PROTECTION WITH THE FEDERAL TRAIT COMMISSION. I WANT TO THANK COORDINATORS, MODERATORS, DIVISION OF MARKETING PRACTICE, DIVISION OF PRIVACY IDENTITY PROTECTION. I WANTED TO OFFER THREE QUICK OBSERVATIONS REGARDING SOME OF THE THINGS WE'VE HEARD ABOUT GOING FORWARD IN COUPLE MINUTES WE HAVE. FIRST, HERE ARE THREE THINGS I PICKED UP. FIRST, THERE MANY OTHERS BUT THEE I WANT TO MENTION. CLEARLY AS PAUL OBSERVED A RANGE OF USE, HOW SERIOUS THE MOBILE MALWARE PROBLEM IS. UNDOUBTEDLY SOME PEOPLE THINK IT'S VERY SERIOUS. OTHERS THINK, MAYBE NOT SO MUCH. SECONDLY THERE SEEMS TO BE LOTS OF OPPORTUNITIES FOR BETTER COMMUNICATION COOPERATION.
DISCUSSION OF PATCHES THAT WE HAD EARLIER TODAY ILLUSTRATED THAT, WE COULD DO A LOT MORE WITH REGARD TO COMMUNICATION AND COOPERATION WE'RE CURRENTLY DOING. THIRD, IT'S PRETTY CLEAR THAT THE U.S. MARKET IS ACTUALLY TAKING GOOD STEPS TO TRY TO SECURE THE MOBILE ENVIRONMENT BUT THAT DOESN'T MEAN WE CAN'T -- WE CAN LET UP. WE HAVE TO CONTINUE TO REMAIN VIGILANT WITH REGARD TO THIS EFFORT BECAUSE YOU KNOW THAT THE HACKERS, THE SCAMMERS, THE FOLKS WHO ARE PUTTING MALWARE OUT THEY'RE GOING TO KEEP TRYING AND PUSHING. WE HAVE TO REMAIN JUST AS VIGILANT. THIS MORNING CHAIRWOMAN TALKED ABOUT THREE THEMES. TALKED ABOUT LAW ENFORCEMENT, EDUCATION AND THIRDLY TALKED ABOUT COOPERATION. SEEMS TO ME THAT FOR PURPOSES OF ADDRESSING THE THREE POINTS I'VE JUST MENTIONED AS WELL AS MANY OTHERS, COOPERATION IS THE KEY. THE FTC IS COMMITTED TO TRYING TO ADDRESS THESE HIGH LEVEL POINTS I MENTIONED AS WELL AS OTHER POINTS I MENTIONED. FRANKLY TO DO SO IN A SENSIBLE WAY, NOT JUST TODAY BUT TOMORROW AND IN THE FUTURE WE NEED THE KIND OF COOPERATION THAT WE'VE SEEN HERE TODAY FROM ALL OF YOU, FROM INDUSTRY FROM, CONSUMER GROUPS WE NEED TO KEEP HEARING FROM YOU, NEED TO YOU KEEP TELLING US WHAT ELSE WE CAN DO TO TRY TO MAKE THIS ENVIRONMENT A BETTER AND SAFER ENVIRONMENT FOR CONSUMERS AND FOR
BUSINESSES.
SO WITH THAT I’D JUST SAY THANK
YOU VERY MUCH.
PLEASE, PLEASE KEEP IN TOUCH
WITH US.
KEEP IN TOUCH WITH OUR
MODERATORS LET US KNOW WHAT ELSE
WE SHOULD BE DOING TO ENSURE THE
CONSUMERS CONTINUE TO USE THIS
WONDERFUL NEW TECHNOLOGY SAFELY
IN WAY THAT WILL BENEFIT THE
MARKETPLACE.
THANK YOU VERY MUCH.