24 COUNTRIES
AUSTRALIA, BRAZIL, CANADA, CHINA, COLOMBIA, DENMARK, FRANCE, GERMANY, INDIA, ITALY, JAPAN, MEXICO, NETHERLANDS, NEW ZEALAND, POLAND, RUSSIA, SAUDI ARABIA, SINGAPORE, SOUTH AFRICA, SWEDEN, TURKEY, UNITED ARAB EMIRATES, UNITED KINGDOM, UNITED STATES OF AMERICA

13,018 ONLINE ADULTS AGED 18-64

EXPERT COLLABORATORS
ADAM PALMER, NORTON LEAD CYBER SECURITY ADVISOR
MARIAN MERRITT, NORTON INTERNET SAFETY ADVOCATE
THE SCALE OF CONSUMER CYBERCRIME
ONE-AND-A-HALF MILLION VICTIMS DAILY

THE GLOBAL PRICE TAG OF CONSUMER CYBERCRIME
US $110 BILLION ANNUALLY

CHANGING FACE OF CYBERCRIME
CYBERCRIME GOES SOCIAL AND MOBILE

SECURITY IQ: MIXED REPORT CARD FOR CONSUMERS
CONSUMERS WISE UP TO TRADITIONAL THREATS, BUT MANY STILL UNAWARE AS TO HOW CYBERCRIME IS RAPIDLY EVOLVING

STRONG PASSWORDS ARE KEY
EMAIL A POTENTIAL GATEWAY FOR CYBERCRIMINALS
THE SCALE OF CONSUMER CYBERCRIME

556 MILLION VICTIMS PER YEAR
MORE THAN THE ENTIRE POPULATION OF THE EUROPEAN UNION

1.5+ MILLION VICTIMS PER DAY

18 VICTIMS PER SECOND
2/3 online adults have been victims of cybercrime in their lifetime.

46% victims in past year.

Close to half of online adults have fallen victim to attacks such as malware, viruses, hacking, scams, fraud & theft.
THE GLOBAL PRICE TAG OF CONSUMER CYBERCRIME

$110 BN

THE COST AMERICANS SPEND ANNUALLY ON FAST FOOD

85% OF DIRECT FINANCIAL COSTS ARE A RESULT OF FRAUD, REPAIRS, THEFT & LOSS

USD $197

AVERAGE COST PER VICTIM

ENOUGH TO BUY A WEEK’S WORTH OF NUTRITIOUS FOOD FOR A FAMILY OF FOUR IN THE UNITED STATES
THE GLOBAL PRICETAG OF CONSUMER CYBERCRIME

ALL AMOUNTS IN USD

- USA: 21 BN
- Mexico: 2 BN
- Brazil: 8 BN
- Europe: 16 BN
- Russia: 2 BN
- China: 46 BN
- India: 8 BN
- Japan: 0.5 BN
- Australia: 2 BN

ALL AMOUNTS IN USD
CHANGING FACE OF CYBERCRIME: CYBERCRIME GOES MOBILE

AS CONSUMERS GO MOBILE, SO DO CYBERCRIMINALS

2/3 OF ADULTS USE A MOBILE DEVICE TO ACCESS THE INTERNET

2X MOBILE VULNERABILITIES

MOBILE VULNERABILITIES DOUBLED IN 2011 FROM 2010*

31% OF MOBILE USERS RECEIVED A TEXT MESSAGE FROM SOMEONE THEY DIDN’T KNOW REQUESTING THAT THEY CLICK ON AN EMBEDDED LINK OR DIAL AN UNKNOWN NUMBER TO RETRIEVE A “VOICEMAIL”

*Symantec Internet Security Threat Report, Volume 17 (April 2012)
CHANGING FACE OF CYBERCRIME: CYBERCRIME GOES MOBILE

...YET IT CAN BE PREVENTED

35% OF ADULTS HAVE LOST THEIR MOBILE DEVICE OR HAD IT STOLEN

2/3 DON’T USE A SECURITY SOLUTION FOR THEIR MOBILE DEVICE

44% AREN’T AWARE THAT SECURITY SOLUTIONS FOR MOBILE DEVICES EXIST
RISKY BEHAVIOR ON POTENTIALLY UNSECURE WI-FI

44% of adults access personal emails via free or unsecured Wi-Fi connections.

GLOBALLY

2/3 of online adults use free public or unsecured Wi-Fi.

53% of those who use free or unsecured Wi-Fi connections are concerned about the security of their connection.
RISKY BEHAVIOR ON POTENTIALLY UNSECURE WI-FI

- 67% ACCESS PERSONAL E-MAIL
- 63% ACCESS THEIR SOCIAL NETWORK ACCOUNT
- 31% SHOP ONLINE
- 24% ACCESS THEIR BANK ACCOUNT
SOCIAL NETWORK USERS REPORT THAT SOMEONE HAS HACKED INTO THEIR PROFILE AND PRETENDED TO BE THEM

SOCIAL NETWORK USERS HAVE FALLEN VICTIM TO CYBERCRIME ON SOCIAL NETWORKING PLATFORMS

BELIEVE CYBERCRIMINALS ARE SETTING THEIR SIGHTS ON SOCIAL NETWORKS

SOCIAL NETWORK USERS HAVE FALLEN VICTIM TO A SCAM OR FAKE LINK ON SOCIAL NETWORK PLATFORMS
LESS THAN HALF
USE A SECURITY TOOL TO PROTECT AGAINST SOCIAL NETWORKING THREATS

1/5
DON’T CHECK LINKS BEFORE SHARING

1/6
HAVE NO IDEA IF THEIR SETTINGS ARE PUBLIC OR PRIVATE

ONLY HALF
USE PRIVACY SETTINGS TO CONTROL WHAT INFORMATION THEY SHARE AND WITH WHOM

1/3
DON’T LOG OUT AFTER EACH SESSION
SOCIAL “FRENEMIES”? 

CONSUMERS ARE ONLY AS SECURE AS THEIR CIRCLE OF SOCIAL NETWORK FRIENDS (INCLUDING FRIENDS OF FRIENDS)

36% have accepted friend requests from people they do not know.

3/10 have received posts or messages that they suspect are not actually from friends.
SOCIAL NETWORK STRESSORS REVEALED

36% of social network users check their social network as soon as they can after waking up.

27% admit that, upon getting to work, they are more likely to check their main social network account than work emails.

16% would end a relationship as a consequence of seeing something they did not like about a person online.

28% feel guilty when they don’t reply to a social network message within a few hours.
**CONSUMERS’ SECURITY IQ**

HIGH MARKS FOR SOME SECURITY FUNDAMENTALS

- **89%**
  - Delete suspicious emails from people they don’t know

- **83%**
  - Have at least a basic antivirus solution

- **78%**
  - Don’t open attachments or links in unsolicited e-mails or texts

Good job!
CONSUMERS’ SECURITY IQ

BUT STILL “ROOM FOR IMPROVEMENT”...

30%
DO NOT THINK ABOUT CYBERCRIME WHEN ONLINE
BECause THEY DO NOT EXPECT THAT IT WILL HAPPEN TO THEM

21%
DO NOT TAKE STEPS TO SECURE THEIR PERSONAL INFO WHEN ACCESSING THE INTERNET
CONSUMERS’ SECURITY IQ

Many online adults don’t know or recognize how viruses or malicious software acts.

40% do not know that a virus or malware can act in a discrete fashion, making it hard to recognize if a computer has been compromised.

49% agree that unless their computer crashes or goes slow, it’s hard to know if their computer is infected with a virus or malware.
CONSUMERS’ SECURITY IQ
AND CONSUMERS DON’T KNOW HOW TO PROTECT THEMSELVES

55% AREN’T 100% SURE THEIR COMPUTER IS CURRENTLY ‘CLEAN’ AND FREE FROM VIRUSES

3/10 DON’T UNDERSTAND THE RISK OF CYBERCRIME OR HOW TO PROTECT THEMSELVES ONLINE

48% ARE ONLY USING BASIC ANTIVIRUS PROTECTION
NEARLY HALF 46% HAVE BEEN NOTIFIED TO CHANGE THEIR PASSWORD BECAUSE THEIR PASSWORD OR PRIVACY WAS COMPROMISED

TOP 3 ACCOUNTS PEOPLE HAVE RECEIVED NOTIFICATIONS TO CHANGE PASSWORDS FOR, FOLLOWING A COMPROMISE:

EMAIL 27%  
SOCIAL NETWORK 19%  
BANK ACCOUNT 15%
STRONG EMAIL PASSWORDS STILL KEY

EMAIL IS A POTENTIAL GATEWAY FOR CRIMINALS LOOKING FOR PERSONAL / CORPORATE INFORMATION

WHAT PEOPLE SEND BY EMAIL:

50% PERSONAL PHOTOGRAPHS
42% WORK RELATED DOCUMENTS AND CORRESPONDENCE
22% BANK STATEMENTS
17% PASSWORDS FOR OTHER ONLINE ACCOUNTS

YET 40% DON’T USE COMPLEX PASSWORDS OR CHANGE THEIR PASSWORDS REGULARLY
WHO IS AFFECTED MOST BY CYBERCRIME?

HIGHEST NUMBER OF CYBERCRIME VICTIMS FOUND IN:
- Russia: 92%
- China: 84%
- South Africa: 80%

CYBERCRIME VICTIMS MORE LIKELY TO BE:
- Male: 71% (compared to 63% of females)
- Millennial: 75% (compared to 56% of Baby Boomers)

AND:
- Mobile Internet Users
- Social Network Users
CONCLUSION

$110 BILLION

THE COSTS OF CYBERCRIME ARE CRIMINAL: $110 BN LOST IN JUST 12 MONTHS.

556 MILLION VICTIMS

1.5M ADULTS BECOME CYBERCRIME VICTIMS EVERY DAY - THAT’S 18 VICTIMS PER SECOND.

CHANGING FACE OF CYBERCRIME

MORE ONLINE ADULTS THAN LAST YEAR INDICATED THAT THEY HAVE FALLEN VICTIM TO NEW FORMS OF CYBERCRIME SUCH AS THOSE FOUND ON SOCIAL NETWORKS OR MOBILE DEVICES – A SIGN THAT CYBERCRIMINALS ARE STARTING TO FOCUS THEIR EFFORTS ON THESE INCREASINGLY POPULAR PLATFORMS.

CONSUMERS DON’T RECOGNIZE CYBERCRIME HAS CHANGED

HALF OF ONLINE ADULTS DON’T KNOW OR RECOGNIZE HOW MALWARE OR CYBERCRIME ACTS HAVE EVOLVED AND DON’T KNOW HOW TO PROTECT THEMSELVES. CYBERCRIMINALS’ METHODS HAVE CHANGED – NOT ONLY DO THEY WANT TO AVOID DETECTION FOR AS LONG AS POSSIBLE, THEY’RE CHANGING THEIR TACTICS TO TARGET FAST GROWING MOBILE PLATFORMS AND SOCIAL NETWORKS WHERE CONSUMERS ARE LESS AWARE OF THE SECURITY RISKS.

STRONG PASSWORDS KEY

EMAIL ACCOUNTS CAN BE A GATEWAY FOR CRIMINALS LOOKING FOR PERSONAL AND CORPORATE INFORMATION, WITH PEOPLE SENDING EVERYTHING FROM PERSONAL PHOTOS TO WORK RELATED CORRESPONDENCE TO BANK STATEMENTS AND PASSWORDS FOR OTHER ONLINE ACCOUNTS. AND YET 40% DON’T USE COMPLEX PASSWORDS OR CHANGE THEIR PASSWORDS REGULARLY.
THANK YOU
THE METHODOLOGY DETAIL

STRATEGYONE CONDUCTED AN ONLINE SURVEY AMONG:

13,018 ADULTS

THE SURVEY WAS CONDUCTED IN 24 COUNTRIES (AUSTRALIA, BRAZIL, CANADA, CHINA, COLOMBIA, FRANCE, DENMARK, GERMANY, INDIA, ITALY, JAPAN, MEXICO, NETHERLANDS, NEW ZEALAND, POLAND, RUSSIA, SAUDI ARABIA, SOUTH AFRICA, SWEDEN, TURKEY, UNITED ARAB EMIRATES, UNITED KINGDOM AND UNITED STATES). *

THE SURVEY WAS CONDUCTED IN THE PRIMARY LANGUAGE OF EACH COUNTRY, AND QUESTIONS ASKED WERE IDENTICAL ACROSS ALL COUNTRIES.


THE MARGIN OF ERROR FOR THE TOTAL SAMPLE OF ADULTS (N=13, 018) IS + 0.9% AT THE 95% LEVEL OF CONFIDENCE.

IMPORTANT NOTES:

THE NORTON CYBERCRIME REPORT IS AN ANNUAL REPORT COMMISSIONED BY NORTON BY SYMANTEC AIMED AT UNDERSTANDING HOW CYBERCRIME AFFECTS CONSUMERS AND HOW THE ADOPTION AND EVOLUTION OF NEW TECHNOLOGIES IMPACTS CONSUMERS’ SECURITY. THE RESEARCH WAS CONDUCTED BY STRATEGYONE, AN INTERNATIONAL RESEARCH AGENCY.

1000 ADULT RESPONDENTS WERE INTERVIEWED IN EACH OF USA AND INDIA. THE GLOBAL DATA HAS BEEN WEIGHTED TO ENSURE ALL COUNTRIES HAVE EQUAL REPRESENTATION OF N=500 ADULTS.

* REFERENCES TO 2011 – 2012 DATA CHANGES IS BASED UPON 20 TRACKING MARKETS ONLY: AUSTRALIA, BRAZIL, CANADA, CHINA, FRANCE, DENMARK, FRANCE, GERMANY, INDIA, ITALY, JAPAN, MEXICO, NETHERLANDS, NEW ZEALAND, POLAND, SOUTH AFRICA, SWEDEN, UNITED ARAB EMIRATES, UNITED KINGDOM, UNITED STATES.
DEFINITION OF CYBERCRIME

CYBERCRIME IS DEFINED AS ANY OF THE FOLLOWING ACTIVITIES:

- Computer viruses or malicious software appeared on my computer
- I responded to a forged, ‘spoofed’ or fake email or website which captured my personal details
- I have experienced online bullying, online stalking, hate crime or other form of online harassment
- Someone has hacked into my email account and pretended to be me
- Someone has hacked into my social networking profile and pretended to be me
- I was approached online by someone in an unwanted sexual way
- I responded to online scams
- I experienced online credit card fraud
- I experienced identity theft
- I responded to an unsolicited SMS text message which captured my personal details
- My phone was infected and a text message was sent from my mobile phone without my permission or knowledge that I later had to pay for
- I experienced another type of cybercrime on my cell / mobile phone / tablet device
- I experienced another type of cybercrime on my desktop or laptop computer

SOCIAL CYBERCRIME IS DEFINED AS ANY OF THE FOLLOWING ACTIVITIES ON SOCIAL NETWORKING PLATFORMS:

- I have been harassed or bullied or had inappropriate content posted about me
- I have responded to a forged or fake message or website trying to get my personal details such as passwords, bank account information (I.E., phishing)
- I clicked on a link or a ‘like’ and it took me to a blank page, or reposted itself automatically into my account
- I have fallen for a scam or clicked on a fake link
- I have clicked on a link or ‘liked’ something which has then reposted itself onto my profile

MOBILE CYBERCRIME IS DEFINED AS ANY OF THE FOLLOWING ACTIVITIES:

- I responded to an unsolicited SMS text message which captured my personal details
- My phone was infected and a text message was sent from my mobile phone without my permission or knowledge that I later had to pay for
- I experienced another type of cybercrime on my cell / mobile phone / tablet device
EXTRAPOLATIONS CALCULATIONS

1) OVER 556 MILLION VICTIMS IN 24 COUNTRIES OVER PAST 12 MONTHS:
ONLINE POPULATION FROM CIA FACTBOOK (24 COUNTRY TOTAL = 1,015,861,551.
ONLINE ADULTS PER COUNTRY X % CYBERCRIME VICTIMS PAST 12 MONTHS PER COUNTRY = 556,152,181 (SUM OF 24 COUNTRIES).

2) 18 CYBERCRIME VICTIMS EVERY SECOND / 1058 CYBERCRIME VICTIMS EVERY MINUTE / ALMOST 64,000 PER HOUR / 1.5 MILLION PER DAY IMPACTING OVER 556 MILLION ADULTS IN THE PAST YEAR IN 24 COUNTRIES*
VICTIMS OVER PAST 12 MONTHS (AS ABOVE) 556,152,181 / 365 DAYS PER YEAR / 24 HOURS / 60 MINUTES / 60 SECONDS.

3) CYBERCRIME COST NEARLY $110 BILLION IN THE LAST YEAR IN 24 COUNTRIES
VICTIMS OVER PAST 12 MONTHS (PER COUNTRY) X AVERAGE FINANCIAL COST OF CYBERCRIME (PER COUNTRY IN US CURRENCY).
FIGURE SHOWN IN THE SUM OF ALL COUNTRIES TOTAL COST.