BEHIND OUR DIGITAL DOORS: CYBERSECURITY & THE CONNECTED HOME

Executive Summary

In support of National Cyber Security Awareness Month (October), ESET® and the National Cyber Security Alliance (NCSA) commissioned a survey to better understand the role of cybersecurity in the American household, providing an inside-look into how it is adapting in the digital era of the data breach. Given the simultaneous rise in our number of connected devices and cyber threats, this survey underlined the importance of cybersecurity as a core commitment in our digital lives.

The findings illuminated a knowledge-confidence gap with a range of implications for online safety practices, culture and concerns in the American home. Broadly, the study revealed that Americans are leaving their digital doors unsecured while connected kids and devices are changing parenting techniques, prompting new rules and concerns.

Despite the spite of the fact that one in five American homes received a data breach notification last year and more than 50 percent of those received multiple notifications, 79 percent still feel safe in their connected homes – with almost half (49 percent) showing a remarkably strong sense of confidence. The study also found that more than 40 percent failed to properly secure their wireless routers – the gateway to most digital devices – by not resetting the factory-set default passwords.

Similarly, parents are becoming more engaged in securing their family's digital assets._Three-quarters (75 percent) of American parents have had a "CyberEd" talk with their kids and 90 percent have made at least one rule about using the Internet and connected devices. This evolution of parenting is a positive indicator that cybersecurity is becoming an in-house norm. However, looking closely at the wide range of rules set by parents, many omitted significant protections for passwords, privacy, piracy and basic etiquette. Yet, more than 61 percent of parents showed a surprisingly high level of confidence with their kids' online activities and their abilities to use the Internet and devices safely and securely,

The study showed that Americans are making significant strides in managing their online lives but the sheer number of new, connected devices have changed what it means to keep our digital lives and homes cyber secure. This always-on, always-connected world requires a new, proactive attitude that will allow us to enjoy the benefits of the Internet with the greatest confidence. Appointing the most digitally literate member of the household to make the safety and security of these devices and the way family members use the Internet a regular priority can help make this a reality. This approach advocates for an online security officer in every home – someone who spends time thinking about all the digital components in household, assesses what security systems need fixing or upgrading, determines an action plan in case of an incident and makes cybersecurity discussions a regular part of conversation.

THEMES AND SUPPORTING POINTS

1. A Knowledge-Confidence Gap

Despite recent data breaches and hacker headlines, American homes feel secure from cyber attacks

- When asked how confident they are that their home network and the Internet-connected devices in the home are secure, 79% responded that they felt confidently safe
    - On a scale of 1-5, 49% percent felt strongly and very confident
    - 30% felt confident

American households need to better secure their digital doors. The wireless router represents a major digital entry point for cyber attacks.

- 2 in 5 households - more than 40% - did not change the factory set default passwords on their wireless routers
- Close to 60% did not (48%) or are not sure (8%) if they changed their router username or password in the last year
- 60% set up their wireless routers on their own

Banks and retail establishments are not the only ones affected by data breaches: Americans are feeling them at home, too.

- 1 in 5 American households have received notification that their information has been lost in a data breach
- Of those affected, 56% have received multiple notifications of being data breach victims
- 1 in 5 households have received notification from a child's (or children's) school that their child's information has been lost in a data breach
- 53.8% of those surveyed experienced some kind of negative online security scenario (direct involvement, indirect involvement, passive story following, etc.) in the last 12 months.
    - Among those affected, 43.6% changed their online behavior as a result.
        - Most common actions were increased alertness during Internet browsing (63%) and password change (55.8%).

In homes across America, identity theft is the major safety and security concern online:

- Which of the following safety and security concerns do you have about using the Internet?
    - Becoming a victim of ID theft – 58%
    - Financial information, such as credit card number or banking information, will be stolen – 46%
    - My social security number will be stolen – 43%
    - Someone will access my personal information, such as my home address and cell phone number will be stolen – 20%
    - One of my devices will be hacked, and I will no longer be able to use it – 16%
    - Someone will use information posted about me to commit physical harm, such as knowing I am away for vacation and breaking into my home – 8%
    - My personal medical information – 9%
    - Someone will post something untrue about me that I cannot fix – 8%
    - Someone will post an embarrassing or unwanted picture of my kid(s)– 3%

2. Rapidly Increasing and Expanding Connectivity

Today's households are more connected than ever and the number of connected devices is growing at considerable pace.

- 67% of those surveyed have between 1 and 5 devices at home connected to the Internet, while 30% have 6 or more devices (5%) of households have 11 or more devices).
    - Only 3% of survey respondents have no devices connected to the Internet.
- 30% of those surveyed today have 2-3 more Interned connected devices at home than last year.
- Americans are connecting more things
    - PCs and Laptops are expectedly on top the list: 67%/75% respectively
    - Mobiles come next: Tablets (53%) and Smartphones (65%)
    - TVs and TV set up boxes are a close third with a combined 54%
    - Gaming 38%
- Remote access to the home is a growing trend: more than 1 in 5 households use a mobile device or any kind of app to remotely access or control any devices in the home (i.e., front door lock, video camera, appliance, or thermostat)

From homework and healthcare to banking, interacting with friends or storing family keepsakes, the Internet is an essential, enabling tool in the American home. Top online activities in American households are:

- Banking and Finances: banking (66%); taxes (30%)
- Entertainment: music streaming (39%) social network (74%); gaming (43%); Streaming TV/movies (45%)
- Shopping and ecommerce: Travel (31%); shopping (61%); selling merchandise (20%)
- Storing personal information: videos/photos (38%); music (36%);
- Fitness and health: 16 %
- Work and Homework: homework (21%); work (28%)

3. An Evolution in Digital Parenting

Beyond the birds and bees, American parents are now having a new kind of talk with their kids – CyberEd

- 75% have had a conversation with children in the home about using the Internet safely and securely
- It's an ongoing conversation too: Parents are proving once is not enough by 81% having 2 or more talks in the last 12 months
    - 18% annually
    - 31 % monthly
    - 17 % weekly
    - 33% sporadically
- Cyberbullying or harassment is the top concern for parents (41%), followed by viewing pornography (38%), contact by strangers (38%) and viewing objectionable or age inappropriate content (37%).

American parents seem to be very confident that their children are protected from online dangers

- Almost 60% are confident that they know everything their kid(s) is doing online –
- Of which 35% are very confident

- 64% are confident with what their kid(s) online activities – of which 36% are very confident
- 61% are confident that their kid(s) can use the Internet and devices safely and securely – of which 34% are very confident

Parents need to set better cybersafety rules for their connected kids

- Only 41% require permission before downloading a new app, game or joining a social network
- Only 40% don't allow password sharing with friends
- Only 34% require that children provide all passwords to online accounts
- Only 23% have a device-free dinnertime rule
- Only 25% have rules about allowing devices in the bedroom after a certain time
- Only 30% limit the kind of personal information allowed for posting on social networks
- Only 31% ban downloading pirated content from the Internet such as illegal games, movies or songs.
- Only 40% limit screen time use per day
- Only 37% limit hours during the day the device can be used
- 10% have no rules at all

When cyber rules are broken, digital timeouts are the most common consequence

- Take away devices for a period of time (63%)
- Put stricter time limits on the use of device (12%)
- Limit device use to specific things (i.e., doing homework or other productive work) (14%)
- Don't have consequences related to tech usage for violating tech rules (6%)
- Have tried making rules and enforcing them but this not an effective strategy (2%)

4. Cybersecurity Education

Parents are grading schools on cybersecurity education but schools are yet to excel

- Only 61% are very or extremely confident that their child's (or children's) personal information generated and collected at school is being protected
- 83% believes its either important or very important that their child graduate from high school with the right skills to use technology safely, securely, ethically and productively
- Only 54% say their child (or children) has ever received any instruction in school about the safe, secure or ethical use of technology – leaving almost half, uninformed.
- And only 22% have received any information about or had their child (or children) mention participation in a cyber-challenge or cyber competition?
- 16% have been notified of a data breach at school

Where Americans learn about online safety

- Most households get their online safety information through word of mouth from family and friends (67%) and 54% find this information very or extremely valuable
- Despite breaking news and hacker headlines, only 12% get their information about keeping family safe online from the media

5. At Home with IoT:

We are on the cusp of the Internet of Things but the jury is spilt on the safety and security of IoT products

- American households share roughly the same negative and positive feelings towards IoT security with 25% saying they are confident or very confident that IoT is safe and secure and 27% saying they are not confident or lack confidence.
- That leaves 40% of American households who are undecided – and a huge opportunity for the IoT industry
- Remote access to the home is a growing trend: more than 1 in 5 households use a mobile device or any kind of app to remotely access or control any devices in the home (i.e., front door lock, video camera, appliance, or thermostat)
- The connected car is fast approaching but Americans have legitimate concerns: 13% already own an Internet enabled vehicle but an even larger number (24%) are very or extremely concerned of a car hack

- Americans are connecting more things
    - PCs and Laptops are expectedly on top the list: 67%/75% respectively
    - Mobiles come next: Tablets (53%) and Smartphones (65%)
    - TVs and TV set up boxes are a close third with a combined 54%
    - Gaming 38%

6. Cybersmart Shopping

Shoppers are abandoning their carts due to security and privacy concerns:

- 33% (1 in 3) of those surveyed at one point abandoned a purchase on a website or through a mobile device because of security and/or privacy concerns.
    - Young people are more willing to pull the plug on a purchase due to security concerns than the older ones.
    - 45% answered "yes" in the 18-24 age group vs. 35% in the 35-54 age group and only 24% in the 55-69 age group.
- The most common reason for abandoning a purchase was that too much information was being asked (50% of respondents).

    Other concerns included
    - Couldn't determine if my information was being handled securely – 38%
    - Wasn't sure how the information would be used after my purchase – 28%
    - Couldn't easily find the company's policies on handling personal information– 15%
    - Just didn't feel confident in the transaction – 46%
- For many, abandoning a purchase due to security concerns is a recurring theme (44% of those who abandoned a purchase did it 2 to 4 times in the last year).

Tech gifts top the list:

- Tech gifts will be top of the shopping list during the holidays.
    - Two out of five (30%) plan on buying a technology gift this season.
    - 40% may consider.

Sticking to the familiar:

- Consumers like to stick to large, well-known brands when shopping online.
    - The fact that it represents a well-known brand is by far the most common reason for trusting a particular site during online shopping (48%).
    - The distant second, popular reason for trusting a particular site (29%) is when it allows the use of alternative payments.
- Young people like to select brands where they have also shopped at their physical stores.
    - 42% of those surveyed in the 18-24 age group chose this reason, which is considerably higher than in any other age group.
    - Only 26% of respondents in the 35-54 age group chose the same reason.

Who's keeping the new gifts safe from hackers?

- Who will be responsible for managing security settings after they receive a tech gift?
    - I will - 74%
    - My child/ parent will - 14%
    - I will probably trust the built-in security settings - 13%

7. The Home Office

The Internet continues to connect our personal and professional lives even as the BYOD trend declines

- A combined 51% of respondents connect to work from home (30%) or bringing working devices home and connecting to a home network (21%)

Methodology

Zogby Analytics was commissioned by ESET and NCSA to conduct an online survey of 1433 adults in the US in September 2015. Using trusted interactive partner resources, thousands of adults were invited to participate in this interactive survey. Each invitation is password coded and secure so that one respondent can only access the survey one time. Based on a confidence interval of 95%, the margin of error for 1433 is +/- 2.6 percentage points. This means that all other things being equal, the identical survey repeated will have results within the margin of error 95 times out of 100.