Norton by Symantec

2016 Norton Cyber Security Insights Report

Understanding cybercrime and the consequences of constant connectivity

CONTENTS

HACKERS ARE HONING THEIR SKILLS WHILE CONSUMERS REMAIN COMPLACENT

Our findings show that consumers are growing increasingly aware of the need to protect their personal information online. Unfortunately, many consumers are not motivated to take even simple steps to stay safe online. As hackers continue to hone their skills and adapt their scams to take advantage of people, it's important for them to take action to protect themselves.

76%

of consumers know they must actively protect their information online, but they still share passwords and engage in other risky behaviors.

*****

Despite the growing threat and awareness of cybercrime, consumers remain complacent about protecting their personal information. While there are people who understand that cybercrime is an inevitable circumstance of living in a connected world, human nature is still at play when it comes to dealing with cyber security. Even past victims of cybercrime sometimes fall back into old habits.

The 2016 Norton Cyber Security Insights Report found that victims of cybercrime within the past year often continued their unsafe behavior. In fact, while these consumers were more likely to use a password on every account, they were nearly twice as likely to share their password with others, negating their efforts. Further, 76 percent of consumers know they must actively protect their information online, but they are still sharing passwords and engaging in other risky behaviors.

Globally, ***35 percent*** of people have at least one unprotected device leaving their devices vulnerable to ransomware, malicious websites, zero days and phishing attacks.

35%

40%

Millennials remain the most common victims of cybercrime, with ***40 percent*** having experienced cybercrime in the past year.

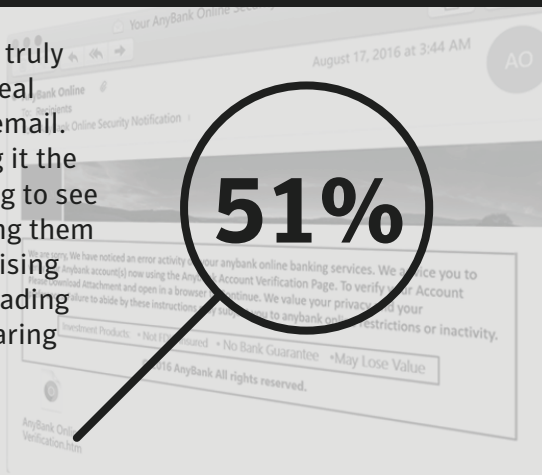
Despite growing up with the Internet, Millennials exhibit surprisingly slack online security habits, and are happy to share passwords that compromise their online safety (35 percent).

MANY CONSUMERS ARE UNABLE TO DISTINGUISH PHISH FROM FRIEND

Phishing scams have been around for more than two decades. In these scams, hackers use email, social media, IMs, text messages and even Internet chat rooms to try to trick consumers into installing malicious software or giving away their financial and social media account information. In fact, hackers have become so sophisticated that consumers still have a hard time identifying the fake emails.

Nearly three in 10 people cannot detect a phishing attack, and another 13 percent have to guess between a real message and a phishing email, meaning ***four in 10*** are vulnerable.

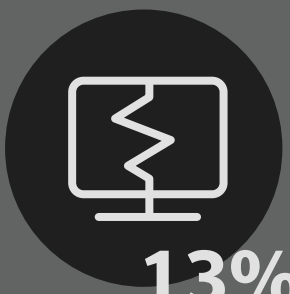
Most people aren't truly sure how to tell a real email from a fake email. ***Only half*** are doing it the right way by looking to see if the email is asking them to take a compromising action, like downloading attachments or sharing their passwords.



86%

Phishing scams will likely remain a popular tactic for cybercriminals. ***Eighty-six percent*** of people said they may have experienced a phishing incident.

Thirteen percent of those people took a compromising action like responding with personal details or clicking links.



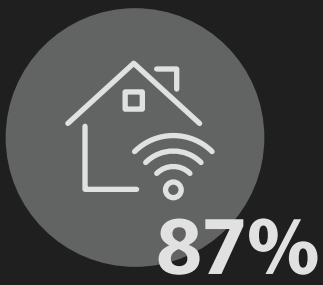
13%

80%

The majority of consumers (***80 percent***) who took a compromising action experienced negative consequences, including identify theft, money stolen from bank accounts, credit cards opened in their name and unauthorized apps installed on their device.

NEED FOR CONSTANT CONNECTIVITY LEAVES CONSUMERS EXPOSED

Consumers are willing to engage in very risky behaviors in order to access Wi-Fi.



Eighty-seven percent of consumers have in-home Wi-Fi.

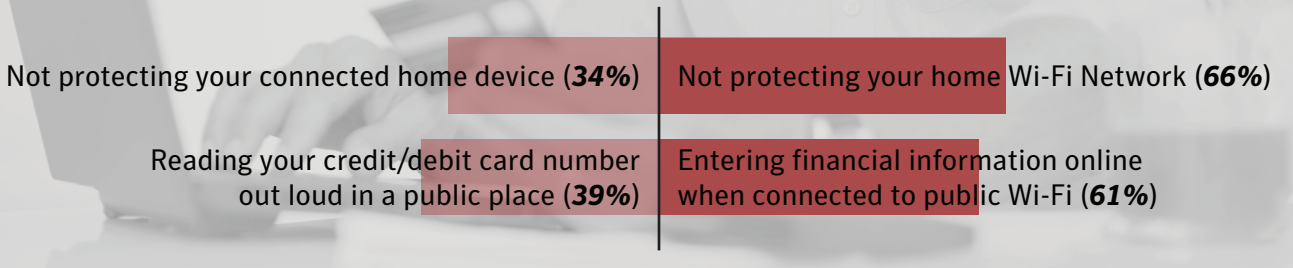
Wi-Fi access is ubiquitous – the vast majority of consumers have Wi-Fi in their homes, and access outside the home is plentiful through coffee shops, airports, libraries and other places where consumers gather. Unfortunately, the benefit of constant connectivity is often outweighed by consumer complacency, leaving consumers and their Wi-Fi networks at risk.

7 in 10
consumers wish they could make their home Wi-Fi network more secure.

yet only
27%
believe it is likely their home Wi-Fi network could be compromised.

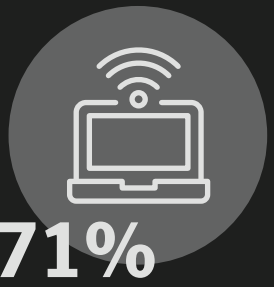
Outside of the home, consumers understand the dangers of public Wi-Fi, but many are not taking action to protect themselves.

EVENT PERCEIVED AS MORE RISKY:



More than one in three consumers don't use a VPN when connecting to public Wi-Fi, leaving them vulnerable to hackers eavesdropping on the network and intercepting the consumer's information. Additionally, if given the option, more than one in five consumers are willing to install a third-party program, like an app, than go without Wi-Fi access.

Considering that ***71 percent*** of consumers say public Wi-Fi is useful for checking emails, sending documents and logging into accounts on the go, this is concerning. If a hacker is able to access an unsecured Wi-Fi network, they can see the information people using the network are sending and receiving from their devices. This means hackers can steal user names, passwords and other personal information they intercept over the unsecured network, putting consumers at risk for identity theft.



OVERCONFIDENCE IN CONNECTED DEVICES IS MAKING CONSUMERS VULNERABLE

As more connected home devices enter the market at different price points, devices such as home security systems, smart thermostats and baby monitors are shifting from "nice to have" accessories to necessary gadgets. With every connected home device purchase, consumers are unknowingly providing hackers with new avenues to launch their attacks. In some instances, poor consumer security habits and vulnerabilities in connected devices are letting hackers into consumers' homes.

44%

of consumers surveyed don't believe there are enough connected device users for them to be a worthwhile target for hackers.

***One in five* connected home device users don't have any protective measures in place for their devices.**

Nearly half (44 percent) of consumers surveyed don't believe there are enough connected device users for them to be a worthwhile target for hackers. Yet, just as hackers learned to benefit from targeting social media and financial accounts, they are on their way to learning how access to connected home devices can be lucrative.

Over six in 10 (62 percent) consumers said they believe connected home devices were designed with online security in mind. However, Symantec researchers identified security vulnerabilities in 50 different connected home devices ranging from smart thermostats to smart hubs that could make the devices easy targets for attacks.

CONSUMERS ADMIT THE RISK IS REAL

The prevalence of cybercrime has merged with people's perception of real-world risks. The associated online dangers – and people's perceptions of those dangers – are even eclipsing real-life threats for some.

Within the last year,

689 MILLION PEOPLE

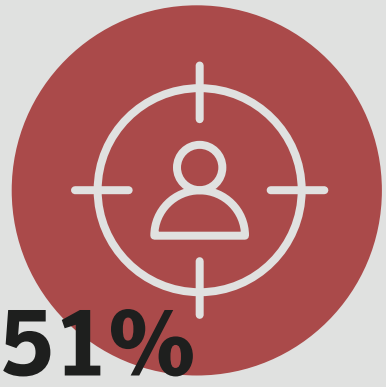
in 21 countries experienced cybercrime.

In the 17 countries surveyed in both 2015 and 2016, we've seen a 10 percent increase since last year.

Since 2015, cybercrime victims spent

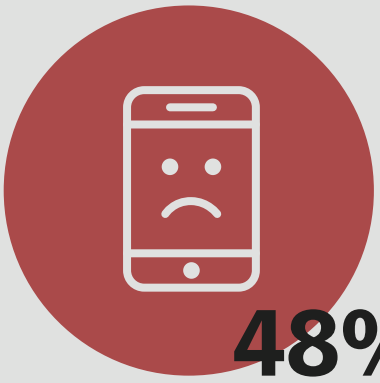
$126 BILLION

globally and spent 19.7 hours dealing with cybercrime.



51%

Fifty-one percent of consumers think it's become harder to stay safe and secure online than in the real world.



48%

Parents are hyperaware of the risks their kids face online. Almost half of parents (***48 percent***) believe their children are more likely to be bullied online than on a playground.

BAD HABITS ARE HARD TO BREAK – ONLINE OR OTHERWISE

Just as we don't leave our front door unlocked when we head out on vacation, we should also not leave our information unlocked online. By adopting a few basic behaviors, we can make big strides in mitigating cybercrime risk. Consider these behaviors to be part of your daily routine like brushing your teeth or wearing a seatbelt.

Avoid password promiscuity: Protect your accounts with strong, unique passwords that use a combination of at least 10 upper and lowercase letters, symbols and numbers to help keep the bad guys at bay. Make it difficult for attackers to access your information by changing your passwords every three months and not reusing passwords for multiple accounts. That way, if a cybercriminal gets your password, they can't compromise all of your accounts. And if it's too overwhelming to keep up with the changes, use a password manager to help!

Don't go on a phishing expedition: Think twice before opening unsolicited messages or attachments, particularly from people you don't know, or clicking on random links. The message may be from a cybercriminal who has compromised your friend or family member's email or social media accounts.

Don't keep a (dis)connected home: When installing a new network-connected device, such as a router or smart thermostat, remember to change the default password. If you don't plan on using the Internet feature(s), such as with smart appliances, disable or protect remote access when not needed. Also, protect your wireless connections with strong Wi-Fi encryption so no one can easily view the data traveling between your devices.

Be in control when online: Entrust your devices to security software to help protect you against the latest threats. Protect all your devices with a robust, multi-platform solution, like Norton Security.

Don't make your private info public on Wi-Fi: Accessing personal information on unprotected public Wi-Fi is like broadcasting your personal smartphone or laptop screen on TV – everything you do on a website or through an app could potentially be exposed. Avoid anything that involves sharing your personal information (paying a bill online, logging in to social media accounts, paying for anything with a credit card, etc.) while on a public Wi-Fi network.

ABOUT THE 2016 NORTON CYBER SECURITY INSIGHTS REPORT

The Norton Cyber Security Insights Report explores the personal impact of online crime. An online survey of 20,907 consumers in 21 markets, commissioned by Norton by Symantec and produced by research firm Edelman Intelligence. The margin of error for the total sample is +/-0.68%. The U.S. sample reflects input from 1,002 U.S. device users ages 18+. The margin of error is +/- 3.1% for the total U.S. sample. Data was collected Sept. 14 - Oct. 4, 2016 by Edelman Intelligence.