Cyber Secure: A look at Employee Cybersecurity Habits in the Workplace

Workers' IT Habits May Be Employers' Biggest Threat

Companies have come a long way in their ability to ward off internal and external cybersecurity threats. However, as the pace of technology innovation speeds up, the threat landscape companies face only becomes more complex. Guarding devices and online data is an ongoing (and always fluctuating) effort. As of mid-October 2015 there were 606 reported data breaches reported, compromising more than 175 million records.[1] It's clear that businesses must make it a priority to protect their own, their customers', and their employees' private information.

Unfortunately, worker cybersecurity knowledge and habits still lag behind. Though some incidents stem from organizations' subpar planning and systems, the majority come from employee error.[2] Being aware of IT best practices isn't enough; cybersecurity is reflected in the many technology decisions employees make daily, whether it's changing logins regularly, avoiding predictable passwords or dodging phishing attempts.[3] In 2014, the Internet Crime Complaint Center received 269,422 complaints with an adjusted dollar loss of more than $800 million. Despite a widespread sentiment that end users are more tech savvy than ever before, reckless behavior persists.

Methodology

To assess the current state of office workers' cybersecurity awareness, CompTIA commissioned an online survey of 1,200 full-time U.S. employees about their regular technology use, cybersecurity awareness and security habits. Simultaneously, CompTIA commissioned a social experiment to more directly observe the behaviors of consumers in real-world settings, to demonstrate how certain activities could lead to IT security risks.

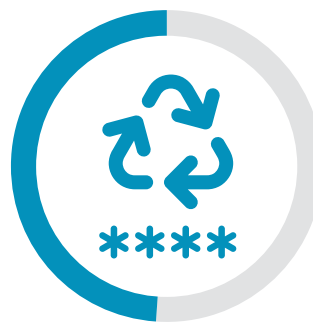## Key findings from the research include:

63%
of employees use their work mobile device for personal activities

94%
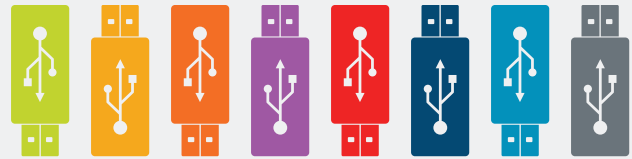of employees connect their laptop/mobile to public Wi-Fi networks

49%
of employees have at least 10 logins, but only 34% have at least 10 unique logins

45%
of employees receive no cybersecurity training from their employers

USB Drop Experiment

One of the most prominent cybersecurity incidents to draw attention to the perils of consumer technology in recent years is "Stuxnet." USB viruses were popularized by this infamous worm, which the U.S. and Israel purportedly used to infiltrate Iranian nuclear centrifuges in 2010. USB sticks programmed with malware can quickly infect devices and critical infrastructure.

From August to October of 2015, CompTIA comissioned a social experiment to observe consumers' cybersecurity habits when faced with found USB sticks. The research team set out to test the hypothesis that, despite the frequency and highly publicized nature of cyberattacks and data breaches, many consumers still exhibit poor security hygiene, unintentionally putting their devices and data at risk.

17%

 of employees plugged the found USB stick into their device

200 unbranded USB sticks were dropped across high traffic public spaces – such as airports, coffee shops and public squares in business districts – including Chicago, Cleveland, San Francisco and Washington D.C. The sticks were preprogrammed with text files prompting anyone who plugged the found USB sticks in to email a specific address or click through a trackable link.

Over the course of a few weeks, 17% of consumers picked up and plugged the found USB sticks into their devices, opened the text file and either clicked the unique link or emailed the listed address. Notably, consumers' technology literacy was not a determining factor for whether a USB stick was picked up or not. At the San Francisco International Airport, for instance, a number of IT industry workers found and plugged in the sticks. In fact, a security office located within a multinational corporation's office building also found a stick and emailed the alias address. In their emails, a handful of respondents asked if the USB had a virus on it, showing that they were willing to jeopardize their devices despite understanding the risks involved. Blindly trusting found USBs – or unprotected Wi-Fi networks, or emails from unidentified third parties – puts more than the individual at risk. As the findings show, even the most IT literate end users can make precarious decisions when faced with potentially suspicious technology, demonstrating how challenging it can be to instill strong cybersecurity habits (not merely knowledge).

Staff Technology Use & Cybersecurity Awareness

The gap between mobile and traditional technology use is closing. A more mobile workforce may be a boon for productivity, but it also creates more endpoints that businesses and end users need to protect. Many employees rely on desktop computers and smartphones for work (78% each), followed closely by laptops (73.5%). Newer technology is quickly making headway, with more than half (54%) of employees reporting regular tablet use and nearly a fifth (20%) using wearable devices to fulfill work duties.

Increasingly, mobile devices intended for work purposes are put to use beyond the office (and beyond actual work). Nearly two-thirds (65%) of employees use their employer-issued mobile devices to work from home, and 61% use them on-the-go in coffee shops, airports and other public settings. Sixty-three percent use their work mobile devices for personal activities, from shopping to using social media to online banking.

Not all employees use technology in the same context, however, and IT departments should be prepared to account for differences in workers' device habits. Men are more likely to use work devices at home (73%) and on the go (68%) than women (59% and 55%, respectively). Millennials (between 21 and 34 years old) are more likely than any other generation to use their devices at home (74%), on the go (73.5%) and for personal activities (79%).

Cybersecurity Perceptions Offer Glimpse Into Cyber Threats Employees Fear Most

Cybersecurity is a catchall for a myriad of IT events, actors and practices. Employees' impressions of cybersecurity vary, and offer a glimpse into the risks and threats workers fear most. At the same time, there's a gap between workers' cybersecurity perceptions and firsthand experiences.

Employees are twice as likely to associate cybersecurity with "identity theft" (36%) than "hacker" (18%); only eight percent connect it with "malware."Nearly one-fifth (19%) of workers claim that their personal information has been hacked in the last two years, despite evidence to the contrary. The Ponemon Institute found that 47% of American adults were hacked in 2014 alone.[4] Roughly one-third (32%) have had a device they use for work become infected in the last two years. Millennials are even more likely to have dealt with a data breach (27%) or infected device (42%).

In the event of a breach, most employees are inclined to take action themselves or contact their IT department. More than one-third of employees would change all of their device and account credentials if hacked – a logical choice, given that many employees reuse passwords for multiple services – while one-fifth would change the credentials only for the affected account. One-third of employees also would contact their IT department to address the situation.

Employees' First Response in the Event of a Virus or Hack

35% change all device and account login credentials

33% contact their corporate IT department/helpdesk

20% change the login credential for the affected device/account

4% contact the police

3% contact a significant other or relative

Though employees are largely aware of the risks of poor cybersecurity habits, many don't apply that knowledge. Workers' overall IT behaviors, from Wi-Fi connectivity to online account maintenance, reflect a degree of vulnerability that malicious actors can easily exploit.

Connecting to Public Wi-Fi Prevalent Among Employees

Employees continue to connect their devices to unprotected Wi-Fi networks in spite of the inherent security risks. Almost all (NET 94%) employees connect their laptop or mobile devices to public Wi-Fi networks, and 69% of this group handles work-related data while doing so. Perhaps due to the lifelong ubiquity of technology for younger workers, the likelihood of connecting to unsecured wireless networks negatively correlates with age.
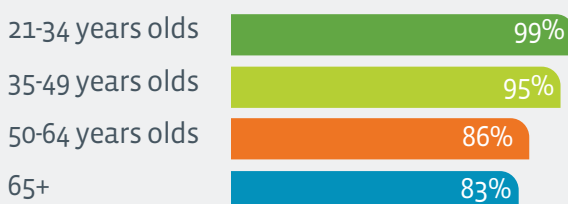
Likeliness To Use Public Wi-Fi Declines With Age

Connect laptop to public Wi-Fi

21-34 years olds	98%
35-49 years olds	94%
50-64 years olds	89.5%
65+	73%
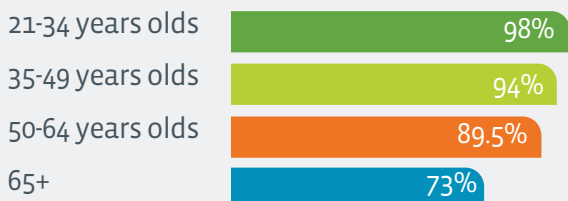
Connect mobile to public Wi-Fi

21-34 years olds	99%
35-49 years olds	95%
50-64 years olds	86%
65+	83%

Even more concerning, many end users connect to unsecured networks when handling sensitive personal and corporate data. The top activities users perform while on public Wi-Fi run the gamut from relatively benign to the objectively risky.

Top Activities Performed On Public Wi-Fi

- **82%** Surfing the web
- **78.5%** Checking work email
- **70%** Using social media
- **60%** Accessing work documents
- **45%** Online banking
- **41%** Purchasing products with a credit card

## Consumers Practice Poor Password Habits

We're in the middle of a password bubble, and employees' account management hygiene has struggled to keep pace. In an environment where workers are encouraged to oversee a growing collection of online accounts – while reusing the same passwords – the defenses around personal and corporate data inevitably start to deteriorate.

Half (49%) of workers have at least 10 account logins, but only a third (34%) have at least 10 unique username and password combinations. Further, 36% use their work email address for personal accounts, while 38% use work passwords for personal accounts. Taken together, this means that some workers are repurposing their work account credentials across multiple personal services. This generates more points of exposure for an organization, and can be difficult to address without better training to spur behavioral changes.

In regards to account maintenance, workers are generally more careful with corporate data. Employees take a safer approach to refreshing their work passwords than personal logins, but plenty of IT departments would still be troubled to know that 37% do so only annually or sporadically.

Many employees are unaware of the account defenses available to them, and those that are often forego security for convenience. For example, 41% of workers are not familiar with two-factor authentication,

48%
voluntarily apply two-factor authentication
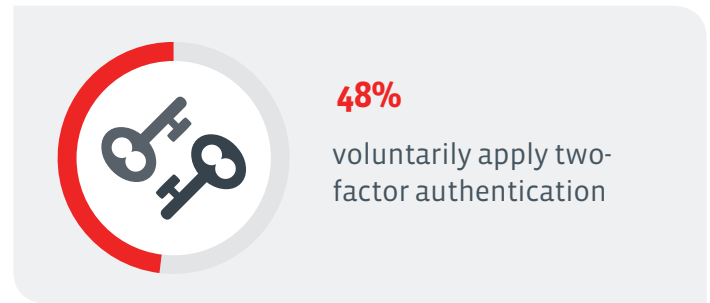
and 27% are familiar with the name but don't understand the concept. Less than half (48%) voluntarily apply two-factor authentication to their accounts.

Regional and age differences play a role in employees' account maintenance habits as well. Employees in the Western U.S. demonstrate the most awareness of two-factor authentication, (38% recognize the term compared to 32% on average), and are also the most likely to apply it to their accounts (55%). Age also factors into awareness: 46% of Millennials are familiar with two-factor authentication compared to 31% of Gen X workers and 21% of Baby Boomers. Similarly, Millennials are the most likely to voluntarily apply two-factor authentication, with 63% participation compared to 51% of Gen X and 34% of Baby Boomers.

Consumers Prone to Sharing Personal Information Online

Many consumers have become conditioned to share at least an email address in exchange for any online content, service or promotion. Generally, workers are comfortable providing their email address, full name and date of birth for a variety of online accounts, making few exceptions across social media, entertainment and e-commerce profiles. Certain pieces of information, however, are more channel-dependent and others are off-limits across the board. Few employees (eight percent) are willing to provide credit or debit card information for social media accounts, but 41% are willing for e-commerce services and 35% for entertainment accounts. Comparatively few (37%) workers would provide a mailing address for a social media account, but nearly three-quarters (71%) are willing to do so for e-commerce purposes, and half for entertainment accounts.

Frequency Of Changing Work And Personal Passwords

|	Work passwords	Personal passwords
Monthly	23%	15%
Quarterly	33%	23%
Annually	9%	14%
Sporadically	28%	40%
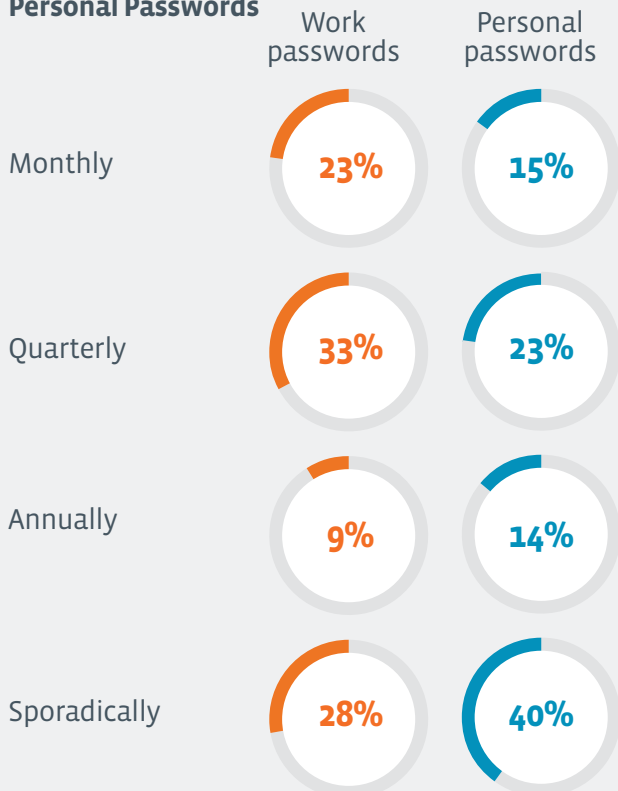
Social Security numbers remain sensitive across all venues; only six percent of employees would share their Social Security number for a social media or e-commerce site, and only five percent for an entertainment account. The same attitude applies to driver's license and identification numbers: only 7.5% would share them for a social media account, seven percent for an entertainment service and nine percent for an e-commerce profile.

Employees and IT Department Share Burden of Protecting Hardware

Safeguarding employees' array of devices is a burden shared by workers and IT departments alike. Unsurprisingly, some employees hold a more stringent hardware protection posture than others.

On a positive note, almost all employees use some form of antivirus program, with only two percent forgoing protection altogether. Most (57%) use paid software, while 30% use free online software and 11% rely on antivirus solutions bundled with their devices.

Antivirus programs used

57%
use paid
software

2%
doesn't use
antivirus
software

30%
use free
software

11%
use bundled
solutions
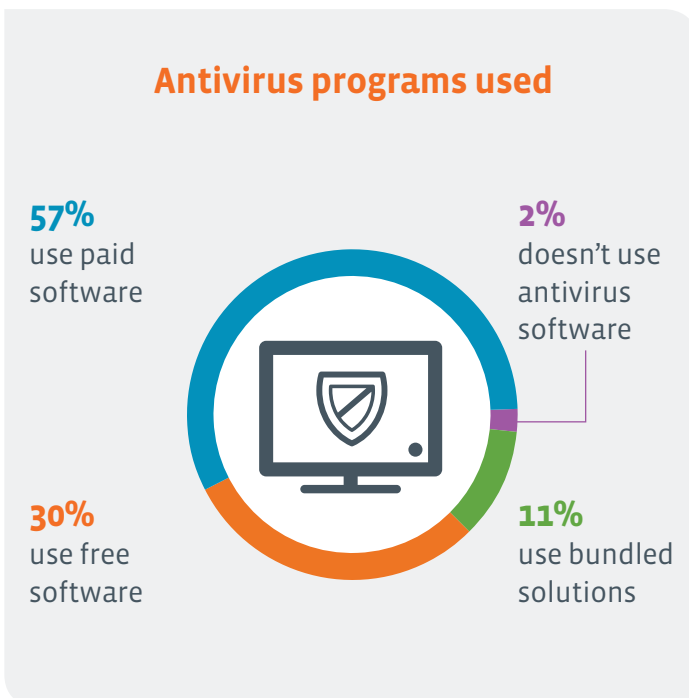
The operating system front is similarly refreshing. Most employees report an active approach to keeping their devices up to date (contrary to the common trope of busy office workers ignoring the "updates available" prompt or snoozing the reminder to avoid an automatic restart.) According to respondents, when IT isn't involved, many strive to stay on top of operating system updates themselves.

Across age groups, Millennials are less likely to have their IT departments manage operating system updates on their work computers, at only 29% compared to 43% of Gen X workers and 46% of Baby Boomers. Millennials are also more likely to implement updates within one week of being prompted (22.5% v. 16% of Gen X and 10% of Baby Boomers).

USB Sticks Not Handled With Enough Care

Despite the proliferation of free and enterprise-grade file sharing apps, not to mention the convenience of email, plenty of employees (58%) rely on USB-based storage drives to transfer files across devices. This presents more than a few security risks, especially given users' propensity for using unfamiliar USB storage devices.

More than one-third (35%) have borrowed someone else's USB stick to copy or transfer a file, while 22% of employees would hypothetically pick up a USB stick they found in public. Of that group, 84% would go so far as to plug the USB into one of their own devices.

Millennials are not only most likely to use USB storage – 74% compared to 55% of Gen X and 47% of Baby Boomers – but also more trusting of found sticks. Forty percent of Millenial respondents are likely to pick up a USB storage device found in public, compared to 22% of Gen X and nine percent of Baby Boomers. Western employees are most likely to use USB sticks, at 63% compared to 56% across South, Midwest and Northeast workers. Western workers are also more likely to pick up found USB sticks, at 28% compared to 22% in the South and Midwest and 19% among Northeast workers.

Cybersecurity Training & Education

45%

of employees report that their organizations don't provide any form of cybersecurity training

Appropriate time to start cybersecurity training for elementary and secondary schools

30% age 5-10

42% age 11-13

Underpinning many of these findings is the reality that many employees don't receive the training necessary to combat cyber risk. Forty-five percent of workers report that their organizations don't provide any form of cybersecurity education, or communicate specific end-user best practices. Organizations that have yet to incorporate IT security into their onboarding and professional development programs are increasingly vulnerable, given how many issue employees devices and entrust staff to handle sensitive corporate data.

Among employers that do administer cybersecurity training, many rely on a mix of online and in-person learning formats.

Perhaps due to adults' widespread lack of cybersecurity education, there's a prevailing sentiment that children should start developing these skills as early as elementary and middle school. Almost one-third of employees feel students' cybersecurity training should begin between the ages of five and 10; 42% believe this exposure should start between the ages of 11 and 13. Less than three percent of respondents claim that cybersecurity is an inappropriate topic for elementary or secondary school curriculum today.
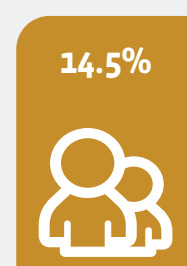
Employers' Primary Cybersecurity Training Methods

32% Online modules

26% In-person group workshops

15% Paper-based training manuals

14.5% 1:1 training

Conclusion

Over the last decade, cybersecurity evolved from a niche concept monitored primarily by governments and corporate IT managers into a mainstream issue commanding above-the-fold headlines and consumer attention. Despite this growing visibility, most employees still demonstrate a lower level of cybersecurity understanding and behavior, both in regards to protecting their devices and their personal information.

Part of this discrepancy may stem from an "IT shepherd" complex. With anti-virus software, firewall protection and other IT protocols installed, employees may feel that anything they do online is safe, or that if something were to happen, the technology would protect them. Not all breaches or identity theft incidents make the headlines, which also may lead some to underestimate their own vulnerability.

At the same time, the ecosystem of consumer technology is swelling, and the lines that once delineated device use are fading. Employees use a variety of personal and corporate tools, but work devices aren't solely used for work purposes (and vice versa.) This blending of data puts the onus on organizations to ensure that employees understand what constitutes "good" cybersecurity hygiene – and are equipped with the skills to demonstrate it.

Today's employers have a long way to go in order to fill the gaps in their cybersecurity training efforts. Business leaders across the HR, IT and executive functions must take a more active approach to educating staff, especially as the threat, software and device landscapes continue to transform. Successful training programs won't simply bestow cybersecurity knowledge or awareness; ultimately they will shape end users' behavior, and prime them to make more informed, safe choices.

In many ways, consumers' tech savvy is greater than ever, but savvy does not always translate to secure. As IT environments become more complex, and the cost of poor protection rises, consumers need to be both.

Methodology

This research was conducted by The Blackstone Group, using an online panel from Instantly, Inc. The panel included 1,200 people who are employed full-time in the U.S. and use a computer at work. Surveys were conducted from September 10 to September 16 using an online platform, and quotas for age, gender, and company size were applied to ensure results were representative across the U.S. workforce.

Sources

1. "Data Breach Reports," Identity Theft Resource Center. September 29, 2015.
   http://www.idtheftcenter.org/images/breach/DataBreachReports_2015.pdf

2. "Trends in IT Security," CompTIA. March 2015.
   https://www.comptia.org/resources/trends-in-information-security-study

3. "2014 Internet Crime Report," Federal Bureau of Investigation. May 2015.
   https://www.fbi.gov/news/news_blog/2014-ic3-annual-report

4. "Half of American adults hacked this year," CNNMoney. May 28, 2014.
   http://money.cnn.com/2014/05/28/technology/security/hack-data-breach/

ROYAL IT