mimecast

Company-issued Computers:

What are employees really doing with them?

Introduction

Now more than ever, organizations are issuing computing devices – laptops, mobile phones, desktops – en masse to their staff. There was no choice, as in March a certain submicroscopic infectious agent arrived uninvited to obliterate 2020.

For so many organizations around the world, one day in March was the last day in the office for a very long time. And this is still the case for many. Work from home (WFH) is the reality for those businesses that can. And to do that efficiently and (somewhat) securely, the issuance of laptops and other computing devices quickly became IT job #1! According to IDC, PC shipments[1] popped to 72 million units in the second calendar quarter of 2020, an 11.2% year-over-year growth.

But have you ever wondered what your employees are doing on these devices? All business of course. Raise your hand if you believe that! Were your IT and security policies and systems ready for this rush to WFH? Do you think the blurring of business and personal lives has increased or decreased in 2020? We had our own guesses and suspicions, but to help answer these questions with some hard data, Mimecast sponsored research in September 2020 of more than 1,000 businesspeople around the world that have a company-issued computing device. Read on to learn what we discovered about what employees are actually doing with these company owned devices.

[1] IDC Press Release, Traditional PC Shipments Continue to Grow Amid Global Economic Slowdown, July 2020

In addition to working remotely, what else is your staff doing on their corporate-issued devices?

The survey results are very clear. Employees extensively use company-issued devices for personal matters. Seventy-three percent of the respondents admitted to it. Big surprise? Not really. This was certainly true when they were on the corporate network too. But now they are doing personal things on their home network using a corporate asset. Unless organizations are consistently driving them through their VPN or a cloud-based secure web gateway, they have little or no visibility to this activity. Is it safe?

73%

of respondents extensively use company-issued devices for personal matters

What are your staff's favorite personal applications?

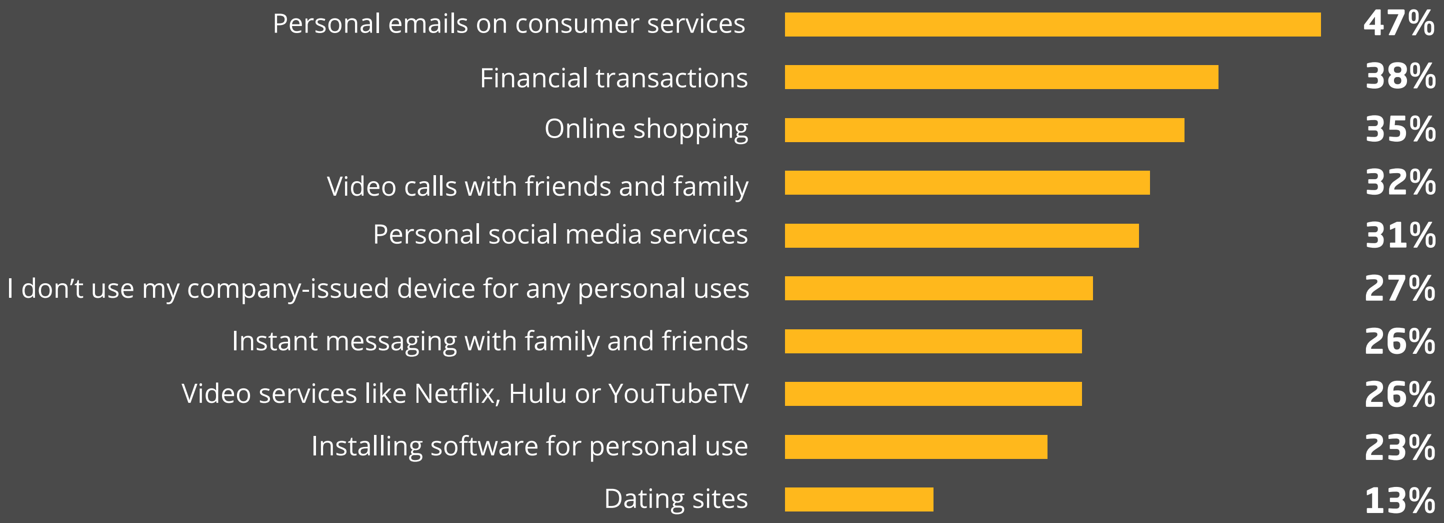
Again, no surprises here. In the order of popularity: personal email (47% of respondents), financial transactions (38%) and online shopping (35%). Well, maybe the only surprise is that these aren't 100% across the board! Not far behind these top three are: social media, instant messaging, video streaming and downloading software for personal use (yikes!). Last but not least, are dating applications.

47% personal email

38% financial transactions

35% online shopping

Top areas of personal use of corporate devices



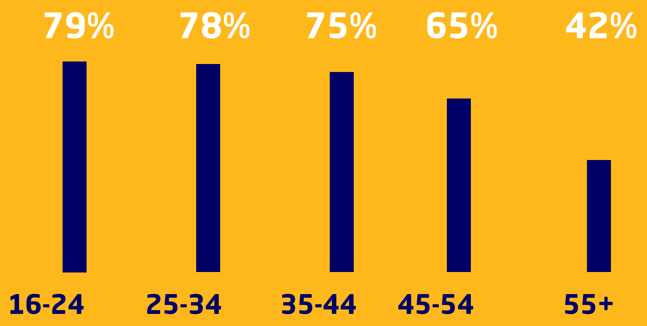
Do men behave differently than women, in the context of this topic?

78% of men report using their corporate device for personal business versus 65% of women.

78% 65%

Do teenagers and 20 somethings act differently than the 55+ cohort?

79% of the 16-24 age group reported using their issued computing devices for personal business, whereas this percentage drops to 42% for the older, 55+ set. Any surprise that the younger crowd blurs their business and personal lives more than their grey-haired elders?



Would you expect any differences in personal use by country of residence?

Start by channeling your view of typical Americans and Australians as compared with typical Germans. No, not cowboy hats and lederhosen. It is worth a mention that respondents from the United Arab Emirates (UAE) need to be included here as notably above average. The UAE “wins” the day on the use of company-issued devices for personal use with 87% responding “yes.” The Americans and Australians trailed a bit at 79% and 78% respectively, both significantly above the 73% average across all respondents globally. In contrast, the German respondents clocked in at “only” 58%.

87% United Arab Emirates

73% Average across all respondents globally.

79% United States

78% Australia

58% Germany

Has the personal use of corporate-issued devices increased with COVID and work from home?

Yes, results suggest that COVID and the rush to WFH had an impact on the amount of personal use of corporate devices. Sixty percent of respondents reported an increase in personal usage during the pandemic, with men again above the average at 65% reporting an increase versus 53% of women.

60%

of respondents reported an increase in personal usage during COVID

How much time on average are employees spending on their company devices for personal business?

Of course, only outside normal working hours! The reported average came to almost 2 hours each day (1.9 hours/day). The results ranged from less than 30 minutes to more than 4 hours a day. How does this compare with the screen time that Apple iOS reports to you on a weekly basis? Do we ever take our eyes off screens? Perhaps we are well on our way to becoming the humans presented in Disney Pixar's movie, WALL-E.

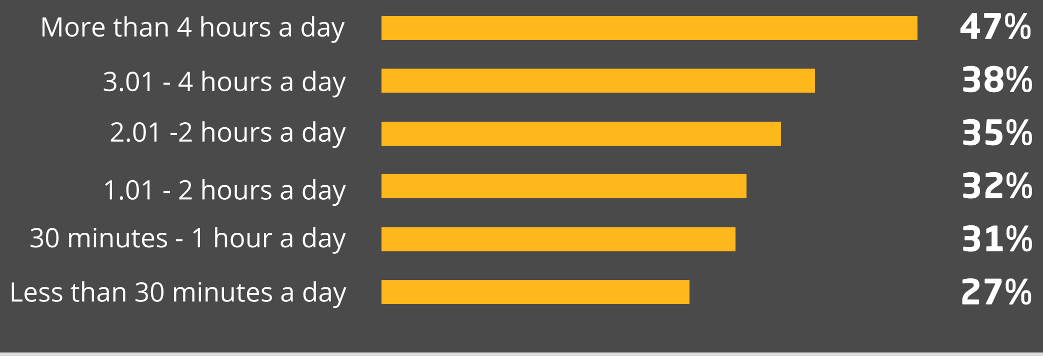
But what about organizations' formal acceptable use policies (AUPs)? Those written policies define what you can and can't do with corporate assets. Does this heavy personal use violate these policies? What about the types of sites that are being visited? Are they all safe and appropriate for business? We don't know the answer to those questions, but we know that 68% of respondents reported that their organizations have AUPs. Maybe many of those AUPs need to pivot with WFH times?

1.9 h/d

the average hours/day correspondents use company devices for personal business

How does this compare with the screen time that Apple iOS reports to you on a weekly basis?

Personal use of corporate devices per day

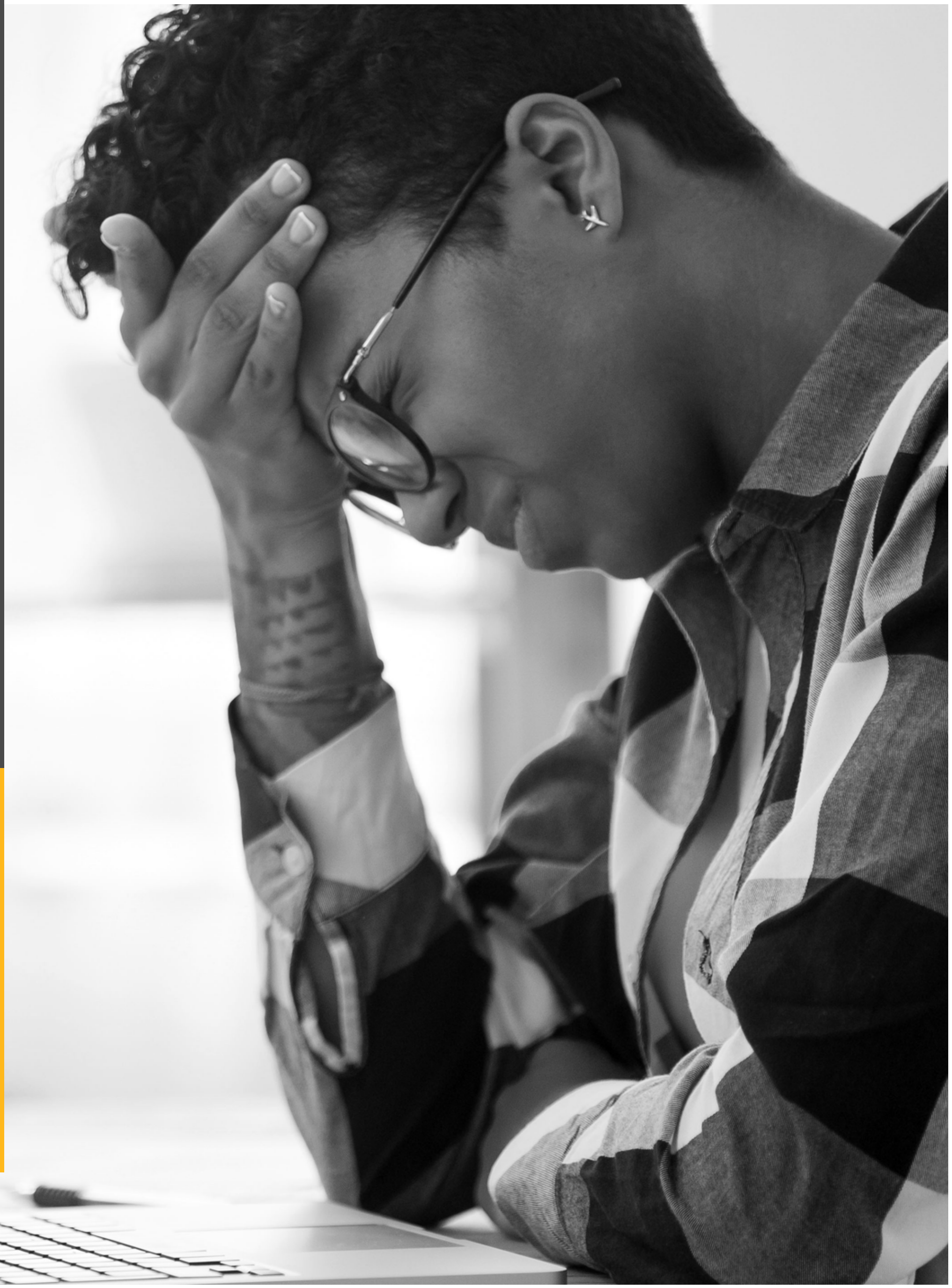


Are employees aware that clicked links could infect their devices?

Fortunately, people are very aware of the risk that links found in emails, on social media and within websites can infect their devices. In fact, 96% of respondents claim to be are aware of this. Americans and Emiratis are even more aware of these risks than average, clocking in at 98% and 100% respectively. But does this near ubiquity of risk awareness greatly reduce respondents' likelihood of opening and engaging with what they consider to be suspicious emails? No.

96%

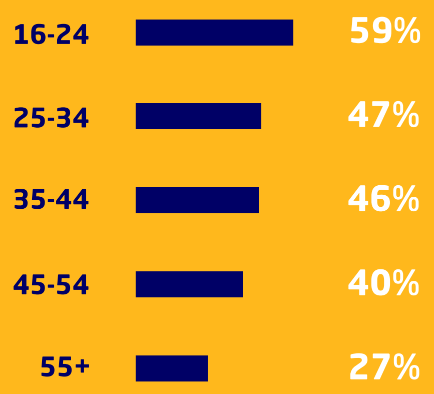
of respondents claim to be aware of the risk



45% of respondents admitted to opening emails they considered to be suspicious

Overall, 45% of survey respondents admitted to opening emails that they considered to be suspicious. And yes, younger folks – 59% for the 16-24 age group – are much more likely than the older set – 27% for 55+ – to open suspicious emails. Who says older people aren't as savvy online as the younger set!

Have you ever opened a suspicious email? (%YES)



34% Brits & Germans opening suspicious emails

And those from the UK and Germany show a relatively high level of savvy compared with other countries to "only" 34% of each opening suspicious email.

60% Americans opening suspicious emails

61% Emiratis opening suspicious emails

Unfortunately, Americans and Emiratis took the "crown" here as well at 60% and 61% respectively, engaging with suspicious emails.

And a congratulations of sorts goes to the public/education sector, which was notably below average - in a good way! - at only 26% opening suspicious emails.

Good job to those showing more caution than average!

26% of public sector and education sector respondents open suspicious emails

Given nearly everyone is so aware of the risks of funky emails, certainly they at least consistently report these suspicious emails to their IT or security departments, right?

Not so much. In fact, 45% of respondents admitted to not reporting suspicious emails to their IT or security teams. But at least the majority do consistently report - though at 55%, it's barely a majority.

👍 **55%** reporting

👎 **45%** not reporting

35% **51%**

Again, showing off their higher risk tolerance (or is it a judgement issue?), men clocked in at 51% who don't consistently report versus 35% for women.

24% **51%**

Keeping consistent with previously discussed statistics, the youngest cohort (16-24) clocked in at 51% versus only 24% for the 55+ age cohort – reporting, not reporting.

36% Germans

55% Amercians

And sure enough, again the USA and UAE take top honors and are neck-in-neck in the lead for non-reporters – 55% and 50% respectively.

Warning to phishers: if you send a phishing email to a German employee there is a better than average chance that if they notice it, they will report it, with only 36%.

Why this gap between very high awareness and notably lower reporting?

Maybe it is a lack of understanding. Certainly, awareness and understanding aren't the same thing. Perhaps it is a process issue, where organizations don't have an easy or well-known way to report such suspicious emails. Or everyday employees just don't think security is their job. Or maybe everyday employees are just too busy dealing with their own WFH challenges.

During the pandemic organizations *are* trying to improve their employees' security awareness

Sixty-four percent of survey respondents report receiving specialized WFH related cybersecurity training in recent months, with the USA and the UAE again in the lead at 78% and 81% respectively. When it comes to security awareness training related to WFH, the Germans lagged at only 37%.

Why is the receipt of security training inversely correlated with good security related actions (clicking on and reporting suspicious emails)? Why do people do (or not do) what they do? A key factor is ineffective security awareness training. We think most security awareness training is not engaging, timely, relevant or motivating for the typical employee. Without proper attention and curation, security awareness training can become just another "check-the-box" activity that has little impact on the organization's security posture.

64%

of respondents report receiving specialized WFH cybersecurity training

Key Takeaways and Recommendations

01: Plan

Assume your staff is going to use their corporate-issued devices both for personal and business use and plan your security strategies accordingly. The outright banning of personal use is probably unrealistic for most organizations.

02: Harden

Harden the devices to make sure unapproved software cannot be installed or rogue devices can't be connected. Generally, don't let your staff have administrative privileges for their corporate-issued devices.

03: Cloudify

Assume your devices will be operating on a hostile network, attempting to browse malicious websites, receiving phishing attacks and trying to download malicious files. Cloud-based security controls were designed specifically to provide high-levels of security no matter from where the user is operating. Requiring everyone to VPN back into the home office just for security purposes is expensive, cumbersome, and typically inconsistently executed.

04: Train

Continue to work on your security training and security culture shift, particularly with the younger demographic. If your training is delivered less often than monthly, takes more than 5-10 minutes a pop and isn't heavily video based, it is old school (read: ineffective) and needs to change immediately.

05: Test

Test your people regularly with simulations to see how well they are doing at spotting cyberattacks like phishing. When possible, use attacks that have actually been directed at your organization to make the simulations as real as they can be.

06: Report

Make sure you have a clear and easy process for reporting suspicious emails and other security relevant activity, such as with an easy to remember email address like security@yourcompany.com. And of course, have the security people and processes to triage these reports as they role in.

Survey Methodology

- Executed by Censuswide
- Data collected in September 2020
- 1,105 respondents
- Countries included: UK, USA, Australia, South Africa, Netherlands, Germany, Canada, UAE
- Organizations with >100 employees
- Respondents currently have a company-issued mobile device, laptop or computer for work
- The survey consisted of the following 8 questions:

Q1. What personal activities, if any, do you use your company-issued mobile device, laptop or computer for?

Q2. During the pandemic, have you been using your company-issued mobile device, laptop or computer more or less often for personal things like shopping, browsing, social media, personal email or other non-work matters?

Q3. How often do you use your company-issued mobile device, laptop or computer for personal use?

Q4. Does your company have a formal policy on personal use of work owned devices?

Q5. Are you aware that links in emails and on social media and websites could potentially infect your device?

Q6. Have you ever thought an email looked suspicious or not quite right but opened it anyway?

Q7. Have you ever received a suspicious looking email but not reported it to your IT or security teams?

Q8. Have you received any special cybersecurity training, specific to working remotely, during the pandemic?

mimecast™

Relentless protection. Resilient world.™

To learn more about effective user awareness check out our Best Practice Guide.

Read now