

Report

# The cyber risks of last-minute holiday deal-seeking



Each year, Kaspersky records tens of millions of phishing attacks and financial Trojans targeting online shoppers and their personal information. With inflationary pressures affecting this year's holiday season, shoppers are projected to be hunting for online deals even more than usual, which could make them more susceptible to scams and malware lurking behind fake online stores and predatory special offers. In order to learn how well-prepared both early and last-minute shoppers are to protect themselves from cyber risks this year, Kaspersky surveyed 2,000 American adults between October 20 and 24 about their holiday shopping and online security habits.

## Key findings



### Last-minute shoppers take more chances

Nearly 1 in 8 respondents (**12%**) said they tend to do most of their Christmas shopping between 12/16 and 12/24.

**40%** of these "last-minute shoppers" are willing to shop on a site that strikes them as sketchy if the offer is enticing enough, compared to just **29%** of early shoppers (those who are mostly done shopping by 12/15).

Last-minute shoppers were less likely to be careful about the information they share online than early shoppers (**44%** vs. **51%**, respectively).

Only **46%** of last-minute shoppers avoid links in messages from people they do not know, vs. 56% of early shoppers.

**33%** of early shoppers follow the recommended advice of using a different password for each online store account, compared to **28%** of last-minute shoppers



### All shoppers face cyber risk

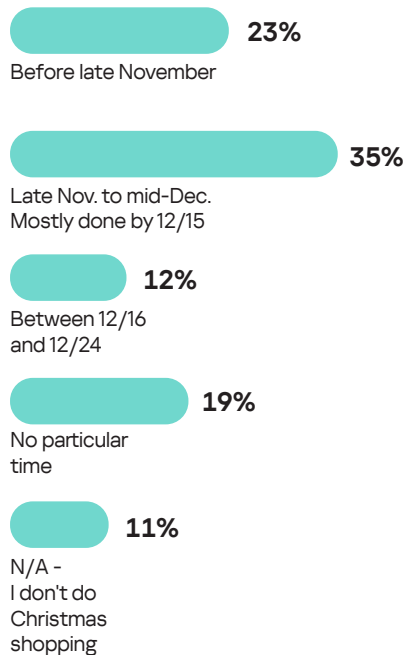
Almost 1 in 5 (**18%**) respondents said inflationary pressures would make them more willing to shop on a site that strikes them as sketchy if the offer is enticing enough.

**38%** of all respondents said they have had credit/debit card details stolen and used fraudulently in the past (not exclusive to holiday shopping).

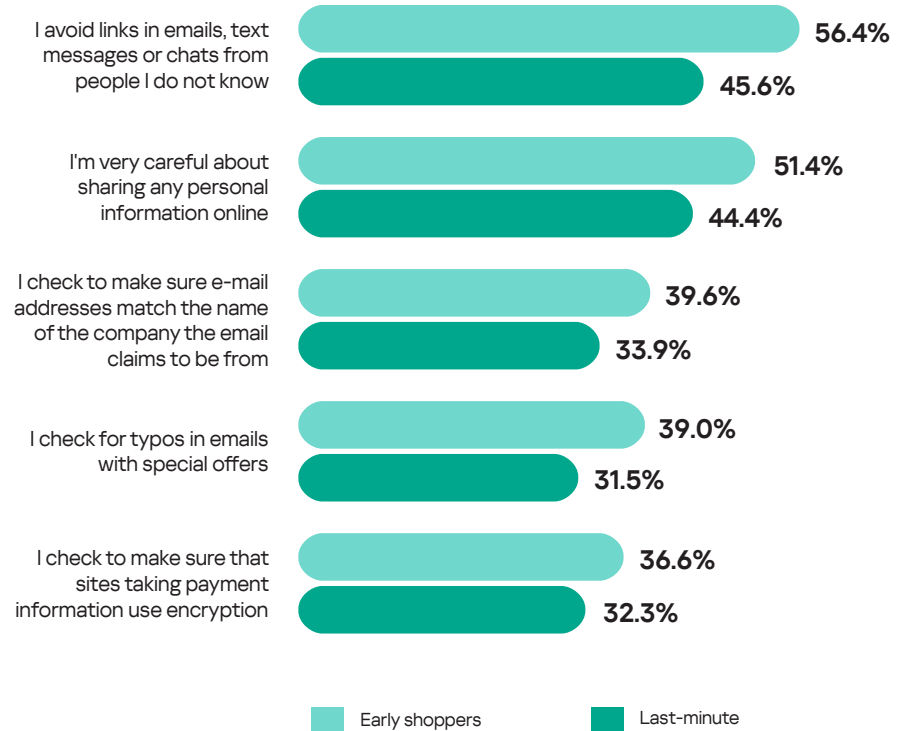
Only **32%** of all respondents typically use a different password for every online account and website that they use for shopping.

**55%** of respondents aged 18-24 are willing to shop on a site that strikes them as sketchy if the offer is enticing enough, compared to just **9%** aged 55+.

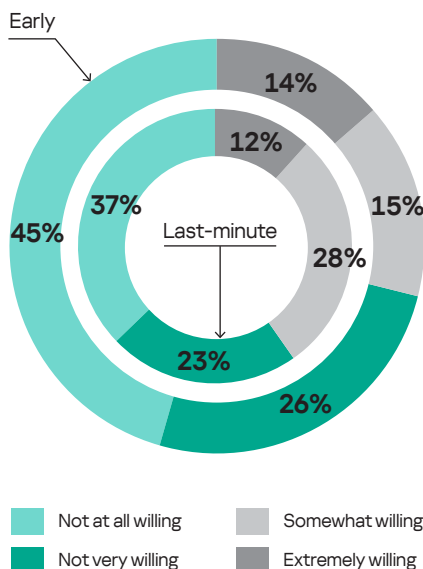
## Typically, when do you tend to do most of your Christmas shopping?



## What do you do, if anything to avoid shopping-related phishing scams? (Check all that apply)



## How willing are you, if at all, to do holiday shopping on a site that strikes you as sketchy if the offer is enticing enough?



“No one loves the holiday shopping season more than cybercriminals, given the elevated level of online transactions, and the fact that deal-seekers often let their guard down and make themselves into vulnerable targets. While much attention is typically given to the Black Friday-Cyber Monday period, the threat of falling victim to scams is always there, especially for rushed shoppers. We urge people to take basic security considerations and to avoid waiting until the last minute, when the time crunch can get them into trouble.”

Kurt Baumgartner,  
principal security researcher,  
Kaspersky

Researchers urge holiday shoppers to leave themselves plenty of time this year in order to help reduce the likelihood that they might fall victim to scams, as well as to take some basic security precautions, such as avoiding password re-use and sticking to official online stores. Shoppers should be wary of phishing scams, too-good-to-be true offers, suspicious links, gift card scams and any offer involving a wire transfer. Experts encourage the use of additional security tools such as antivirus, password managers and VPNs, as well as shopping with credit cards, which generally offer higher fraud protection than debit cards.