FUJIFILM
Value from Innovation

An Evolving Workforce

The work-anywhere setup fits today's continuously transforming industry practices. A research shared by World Economic Forum shows that productivity increased 4.4 percent when employees moved from working at home on a limited basis to the location of their choice*. Being mobile lets individual employees and distributed teams adopt different work processes to deliver results efficiently and flexibly, wherever they may be.

*Work from Anywhere: Geographic Flexibility and Productivity Effects at the United States Patent Office. Harvard Business School and Northeastern University.

Risk Boulevard

A borderless, deskless setup allows workers to be on the move—working from home, working while traveling, or working remotely. But the journey is not without its hazards. Security doesn't stop when a user leaves the office. In fact, it's just the beginning.

The perils of working on the go

Phishing Attacks

Mobile users are more likely to be victims of phishing attacks. 87% of phishing attacks on mobile devices use messaging, gaming, and social media apps as avenues of attack.

Source: Wandera Mobile Threat Landscape Report 2020

Email Breaches

96% of phishing attacks arrive by email. As an email address is often the user login as well, accounts with single-authentication are protected by just the password.

Source: Verizon 2021 Data Breach Investigations Report

Stolen User Credentials

52% of organizations had credentials or accounts compromised according to the 2021 State of the Phish Report.

Source: 2021 State of the Phish Report

Leaked Customer Data

Customer details and info were targeted in more than 53% of data breaches.

Source: Verizon 2021 Data Breach Investigations Report

Additional Threats

Loss of devices or data, mobile malware, data leakage, and Cloud storage breaches

7 Ways to avoid the hazards

1 Use Two-Factor Authentication

Adopt two-factor authentication (2FA). This means a password isn't sufficient for an attacker to breach the system, as two or more pieces of evidence are required to authenticate the user.

2 Establish BYOD Policies

Establish BYOD (bring-your-own-device) policies that allow the organization to control the security on any device users bring to the network, such as remote wiping for lost or stolen devices and auto-locking of inactive devices.

3 Apply Access Rights

Apply individual user-based IT access rights with audit logs for any documents that have been copied, printed, scanned or faxed.

4 Enforce User Rights Management

Set up rights management to reflect user requirements – 67% of all data breaches are caused by user misuse. In the first half of 2020, there was an approximate 35% increase in total attack volume.

Source: Microsoft Digital Defense Report, September 2020

5 Provide Mobile Authentication

Employ mobile authentication and security tokens which are convenient to use

6 Ensure Confidentiality

Ensure document life cycle confidentiality by having decisive control over information sharing, permissible changes or reproduction.

7 Connect to a Secure Cloud Hub

Connect to a secure cloud service hub that centralises document management, including scanning and printing, from multiple popular cloud platforms.

We help maximise the productivity of remote working teams with our seamless, secure cloud and mobile solutions.

Contact your FUJIFILM Business Innovations sales representative now.

FUJIFILM
FUJIFILM Business Innovation New Zealand Limited

www.fujifilm.com/fbnz/

© FUJIFILM and FUJIFILM logo are registered trademarks or trademarks of FUJIFILM Corporation.