NETRUST

SECURING DATA
WHILE WORKING REMOTELY

DATA ACCESSED OUTSIDE AN OFFICE ENVIRONMENT IS AT GREATER RISK

Remote working increases the risk of data breaches due to a lot of data movement outside of the company network and alternate device usage of remote workers. Organizations will have challenges monitoring and controlling data and file movement.

Source: https://www.itgovernance.eu/blog/en/gdpr-the-implications-of-working-from-home-or-on-the-road

FINALCODE

With FinalCode, organizations can protect sensitive files within and outside the corporate network. Information is protected even if shared outside of the organization, lost, stolen, intentionally leaked, and accidentally sent to unintended recipients. Access to the file is controlled – when they can be accessed and what can be done in the file.

INCREASE IN PHISHING ATTACKS WHEN COVID-19 CRISIS STARTED

Attackers are using coronavirus-themed phishing emails and links to steal credentials and distribute malware.

Source: https://www.ncsc.gov.uk/news/covid-19-exploited-by-cyber-actors-advisory

Menlo eliminates all web and email security risks through isolation. Links and web pages are opened in an isolated browser and malicious contents and known bad sites are blocked.

Menlo Security
IT'S SAFE TO CLICK

NETRUST

LACK OF STRONG AUTHENTICATION LEADS TO DATA BREACH

VPN

The sudden move to a work-from-home setup forced some organizations to use VPNs and other remote working tools and software, which are potentially vulnerable due to lack of security measures. Vulnerabilities could allow an unauthenticated attacker to access or steal your data.

Source: https://www.ncsc.gov.uk/news/covid-19-exploited-by-cyber-actors-advisory

IntelliTrust™

IntelliTrust is a cloud-based multi-factor authentication that can provide an additional layer of security to systems and applications. Other features include streamlining VPN access with frictionless authentication, transitioning to cloud SSO, providing seamless and secure login. A wide range of authenticators are available (Push Notification, SMS/Email OTP, QR Code, Soft Token, etc)

SURGE IN MALICIOUS EMAILS

For the last couple of months since the pandemic started, the volume of malicious emails related to COVID-19 have reached 1.5 million daily. One form is an email claiming to be from the World Health Organization (WHO) that sends an attachment that unleashes malware.

Source: https://threatpost.com/cyberattackers-1-5m-covid-19-emails-per-day/154970/

Net-ID offers digital signing of emails to prove the identity of the sender. It can also be used to encrypt email attachments and documents.

NETRUST
Net-ID

NETRUST PHILIPPINES CORPORATION https://www.netrust.com.ph sales@netrust.com.ph
+632 8553-5106 Unit 4G-1 OPL Building, 100 C. Palanca St. cor Dela Rosa St. Legaspi Village, Makati City 1229