A Typical Day in the Life of a Remote Worker

WITH NETRUST SECURE IDENTITY

An employee working remotely turns on the laptop and connects to a Virtual Private Network (VPN) using a username and password. This form of authentication is no longer adequate to keep organization's data safe and secure. Using single authentication for remote working increases the risk of security breach.

Problem Solved with NETRUST SECURE IDENTITY

The NETRUST SECURE IDENTITY (embedded in a Cryptotoken) will provide another layer of security. This will be the second form of authentication. Even if user credentials are stolen, cyber criminals will not be able to access the organization's data without the physical device that stores the NETRUST SECURE IDENTITY.

The President (or any C level executive), in the course of a day, will have sent multiple confidential emails to the Board of Directors, and his executive team.

Problem Solved with NETRUST SECURE IDENTITY

Any confidential email can easily be encrypted by the sender using his/her NETRUST Secure Identity (embedded in a cryptotoken) and only those required to read it can have access to these. No email administrators will be able to see these confidential emails even while it sits on the server.

NETRUST

NETRUST SECURE IDENTITY

Protecting your Data. Securing Your Digital Identity

Employees receive tons of emails in a day. Cyber criminals are using the COVID-19 pandemic to steal user credentials and deploy malware. Spear phising is a crime that targets the organization's weakest link: the unsuspecting employee.

Problem Solved with NETRUST SECURE IDENTITY

Once an organization has a trusted SECURE Identity Source (Own Certificate Authority), all emails can be digitally signed. Thus, emails coming from hackers who pretend to be somebody from the Organization can easily be detected by an employee.

An IT Administrator may work with vendor partners when they are exploring to invest on infrastructure or security solutions. With this, they must share confidential data like architectural diagram etc.

Problem Solved with NETRUST SECURE IDENTITY

While these vendors sign NDA, there is still a high chance of the file being compromised unintentionally if the file gets in to the wrong hand if there is no file protection in place. If an employee has a way to encrypt individual files with a password (for external parties) and with NETRUST SECURE IDENTITY for internal parties, these files will remain secure wherever they may be.

An IT Administrator may need to do a remote session via VPN to log in to important systems in the corporate network, as going to the office may not be possible due to current goverment measures in place to contain the spread of coronavirus.

Problem Solved with NETRUST SECURE IDENTITY

Providing access to your network from outside, via VPN, can easily be compromised if you are only using username and password. Using the same NETRUST SECURE IDENTITY on the employee's cryptotoken, the access to VPN is highly secure.
Even if the password was hacked/exposed, one cannot login without the NETRUST SECURE IDENTITY stored in the physical device.

Signing of documents such as agreements, contracts, memos, letters, purchase requisitions, purchase orders, invoices can be a problem for organizations on a work-from-home set up, especially if multiple approvals and signatures are required.

Problem Solved with NETRUST SECURE IDENTITY

With remote working, routing physical copy of documents is a great challenge. In addition, physical signature can be forged. Physical signatures can be replaced with SECURE Digital Signatures using the same NETRUST SECURE IDENTITY. This process of digital signing is supported in PDF. Thus, PDF signing can be done by routing it via email, wherever the signatories may be.

Electronically signed soft copy of contracts and agreements are not protected against data manipulation.

Problem Solved with NETRUST SECURE IDENTITY

The digital data can be easily changed (e.g. from Php 100,000 to Php 1,000,000) using Photoshop. This can be easily denied by the other parties when real malicious intent was planned, as one can claim that he or she did not sign on the document, or what he or she signed was a different figure. If the document is digitally signed using the same NETRUST SECURE IDENTITY, one can verify whether the document is the originally signed document or has been changed.

NETRUST PHILIPPINES CORPORATION https://www.netrust.com.ph sales@netrust.com.ph (+632) 8553 5106