

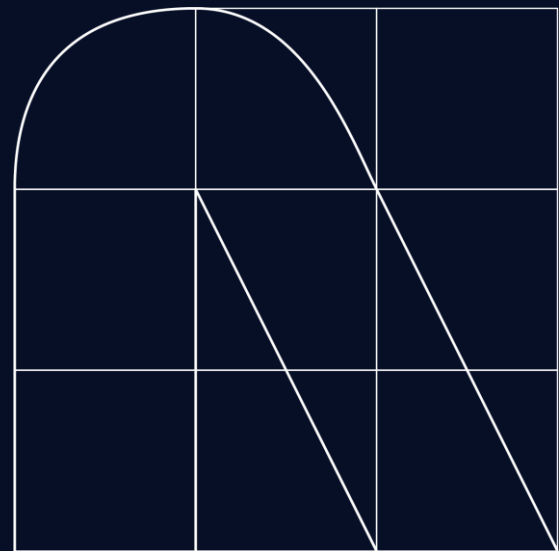


October · Cybersecurity Month

7 Habits for a Safer Digital Life

A short guide to turning good digital decisions into everyday habits.

Security starts with every decision



Cybersecurity is also a matter of habits

Small everyday decisions can make a big difference.

BEFORE YOU START

Security starts with every decision. You do not need to be a cybersecurity specialist to reduce risk. Many of the decisions that protect our information, our identity, and our organization begin with simple actions we repeat every day.

Threats evolve, tools change, and artificial intelligence is making some scams increasingly convincing. But a significant part of security still depends on very human decisions: pausing before clicking, checking an unexpected request, protecting an identity, or speaking up when something does not look right.

This guide brings together seven simple habits for employees and citizens. They are not meant to turn anyone into an expert, but to help people develop better digital judgment and respond more safely to everyday situations.

THE 7 HABITS, AT A GLANCE

- 01 Think before you click.
- 02 Protect your digital identity.
- 03 Verify before you trust.
- 04 Share only what is necessary.
- 05 Keep your digital environment up to date.
- 06 When in doubt, report it.
- 07 Keep your digital judgment sharp.



Pause the impulse. Protect your access

Two foundational habits to reduce risk before it becomes an incident.

01

Think before you click

Many digital scams are designed to trigger an immediate reaction: urgency, fear, curiosity, or the feeling that we need to act before we think. An email, message, or link may look routine and, precisely for that reason, seem convincing.

The most useful habit is to create a brief pause. Before opening a file, following a link, or responding to an unexpected request, look at the context: Were you expecting the message? Is the sender really who they claim to be? Are they asking for something unusual? A few seconds of checking can prevent a decision that is difficult to undo.



PUT IT INTO PRACTICE

Pause for a few seconds and check the sender, context, and request before you act.

02

Protect your digital identity

In the digital environment, our credentials represent who we are and what we are authorized to do. That is why protecting an account is not only about choosing a strong password: it means reducing the chances that someone else can impersonate us.

Use different passwords for different services, enable multifactor authentication whenever available, and never share access codes, even when the request appears to come from someone you know. At work, follow official processes to request or grant permissions. Identity is a gateway; the better we protect it, the harder it is to turn a compromised credential into a larger incident.



PUT IT INTO PRACTICE

Enable MFA and do not share passwords, codes, or access through unofficial channels.



A timely pause and a well-protected identity are two of the simplest—and most effective—decisions we can turn into habits.

Verify. Share thoughtfully

Digital trust is built by checking before acting and reducing unnecessary exposure.

03

Verify before you trust

Artificial intelligence can make a message, a voice, or an image look highly convincing. That is why one of the most important digital skills is separating appearance from trust: something that “looks real” is no longer enough to consider it authentic.

When you receive an unusual request involving money, sensitive data, access changes, or confidential information, verify it through a second channel. A call to a number you already know, a message through the corporate channel, or a direct check may be enough. Verification is not distrust; it is a responsible way to protect people and the organization.



PUT IT INTO PRACTICE

For sensitive or unusual requests, always confirm through a second trusted channel.

04

Share only what is necessary

Security also depends on how much we expose. Every document, data point, permission, or conversation we share increases the number of people and systems that must protect that information. Applying the “need-to-know” principle reduces risk without making work more difficult.

Before sending a file, posting information, or granting access, ask who really needs to see it and for how long. Avoid moving sensitive data to unauthorized channels, and review recipients before clicking “send.” The same is true in personal life: the more we post about routines, travel, work, or relationships, the more context we give those trying to create convincing scams.



PUT IT INTO PRACTICE

Review recipients, permissions, and the channel before sharing information or files.

Keep your environment ready and report quickly

Updating and reporting are prevention and response habits—not tasks reserved for technical teams.

05

Keep your digital environment up to date

Updating is not just about getting new features. Updates fix errors and vulnerabilities that attackers may exploit. Postponing them indefinitely can leave open a door we already know how to close.

Make updating a routine: install system and application updates when appropriate, restart devices when needed, and avoid installing software from untrusted sources. In corporate environments, follow your organization's update policies and do not disable controls simply because they are inconvenient. A well-maintained digital environment is less vulnerable and easier to protect.



PUT IT INTO PRACTICE

Update when required, and use only authorized software and channels.

06

When in doubt, report it

A suspicious message, an unusual login, or even an accidental click should not be hidden. The sooner an organization knows about a potential incident, the more options it has to investigate, contain, and reduce the impact.

Reporting does not mean you have to be certain an attack is underway. It means sharing a signal so it can be assessed. If you opened a suspicious file, entered a password where you should not have, or noticed unusual behavior, use your organization's designated reporting channel as soon as possible. In your personal life, change credentials when necessary and contact the affected service through its official channels.



PUT IT INTO PRACTICE

If something does not look right, report it quickly. Early warning can reduce the impact.

Keep your digital judgment sharp

A strong security culture is built when learning stops being occasional and becomes an ongoing practice.



07

Keep your digital judgment sharp

Threats change because technology, channels, and our own habits change too. Annual training can help, but a true security culture is built when we learn continuously and apply that learning to real situations.

Take part in the security training, simulations, and communications available to you. Pay attention to new types of fraud and share what you learn with coworkers, family members, or people who may have less digital experience. The goal is not to stay on constant alert, but to recognize patterns, ask better questions, and know what to do when an unexpected situation arises.



PUT IT INTO PRACTICE

Review your habits regularly and share what you learn with the people around you.



SEVEN HABITS. ONE IDEA

You do not need to be a cybersecurity expert to make better security decisions. You need to turn them into habits: pause, verify, protect, share thoughtfully, update, report, and keep learning.

SECURITY STARTS WITH EVERY DECISION

Learn how NTT DATA can help you build a stronger security culture through continuous training and learning experiences tailored to your organization.



Contact grupo.hacking@nttdata.com to discover NTT DATA's cybersecurity training platform.

