DO YOU KNOW?

DARK PATTERNS: HOW WEBSITES TRICK YOU

They use "dark patterns"—hidden tricks in design to make you do what they want, not what you want.

CENTRE FOR RESEARCH AND GOVERNANCE ON CYBER LAW

WHAT ARE DARK PATTERNS?

Dark patterns are deceptive design practices used by websites and apps to nudge users into decisions they may not fully understand or intend, such as sharing more data, spending more money, or giving consent unknowingly.

Think of it this way: A website knows what choice makes it more money.

They design the page so that their choice is the easiest and most obvious one to click.

HOW DO THEY WORK?

Dark patterns rely on design tricks like confusing language, visual imbalance, or hidden options to make one choice obvious and the other difficult, even when both should be equally accessible.

YOU'VE SEEN THEM BEFORE

Ever experienced this?

A free trial that quietly converts into a paid subscription?

A pop-up where "Accept All" is bright and bold, but "Reject" is hidden?

An ad you clicked because the "X" button was nearly invisible?

These are classic dark patterns.

COOKIE CONSENT TRICKS

Websites tell you they use cookies and ask for permission. There's usually a big, bright “Accept All” button.

But if you want to turn off cookies? You have to click through multiple menus and manually toggle off dozens of options one by one.

Most people just click "Accept" because the alternative is too confusing.

WHY THEY'RE HARMFUL?

These practices quietly extract data, time, and money, often without users realising the long-term consequences, such as persistent tracking, targeted manipulation, or loss of privacy.

THE LEGAL GAP

While some deceptive sales practices are illegal, dark patterns related to privacy and consent often fall into legal grey areas, particularly where comprehensive data protection laws are absent or weak.

GLOBAL PUSHBACK

Regulators in the **US** and elsewhere have begun treating dark patterns as unfair and deceptive practices, with privacy laws in jurisdictions such as **California** explicitly banning designs that make opting out intentionally difficult.

HOW TO PROTECT YOURSELF?

1. Slow down before clicking. Read labels carefully.
2. If a button looks too tempting to be true, it probably is.
3. Look for the small, quiet option. That's often the one that benefits you.
4. Check settings after signing up for anything.
5. Never assume the default is the right choice. Defaults are chosen to help the company, not you.

Centre for Research and
Governance on Cyber Law

Empower Yourself—
Know Your Digital Rights!

Share this post to spread awareness.
Follow CRGCL for more updates on digital governance and cyber law.

www.crgcl.com