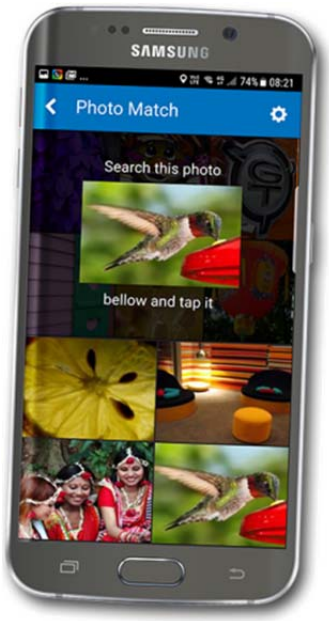
Protect your staff and users against their greatest security threat:

Themselves.

CryptoPhoto's simple user interface protects people against phishing, social-engineering, spoof sites, and other confidence trickery, while our technology neutralizes malware, sophisticated man-in-the-middle attacks, server-side break-ins, and more. 91% of real-life cyber break-ins and theft are caused by the people-problems that CryptoPhoto blocks.



Simple at first glance. Sophisticated inside.

We use visual mutual-authentication to keep people safe while making their logins ultra-fast and easy. This useability advantage is unique: before now, higher-security has never been delivered in a faster and easier package. The seeming simplicity of our user-experience masks our high level sophistication and threat-blocking technical advantage: it's all there, but it wastes nobody's time while it works.

What is Mutual-Authentication, and why is it important?

Ordinary authentication is when a person proves their legitimacy to a computer. Mutual-authentication enhances this into a two-direction process, where the computer **proves** its own legitimacy to the person at the same time.

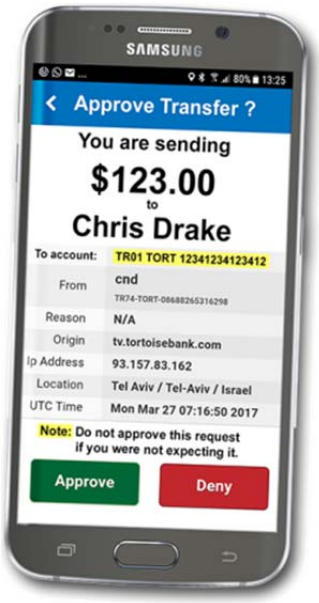
This is important, because without trust at **both** ends of the authentication process, imposters and trickery make it possible to steal credentials or deceive victims. Mutual-authentication blocks this, because only the real computer is able to authenticate to the real person.

Except for malware (see next page), every problem that manifests from authentication failure is due to theft of victim credentials or sessions. Mutual-authentication blocks thefts.

Every Channel.

To keep customers safe, your security needs to look after them not just on your website, but also during inbound and outbound phone calls, in person, and in the future of IoT, FinTech and 3rd party access. CryptoPhoto does this all, stopping fraudsters across all channels of attack and preventing security bypass.

What's the difference between Authentication and Signing?



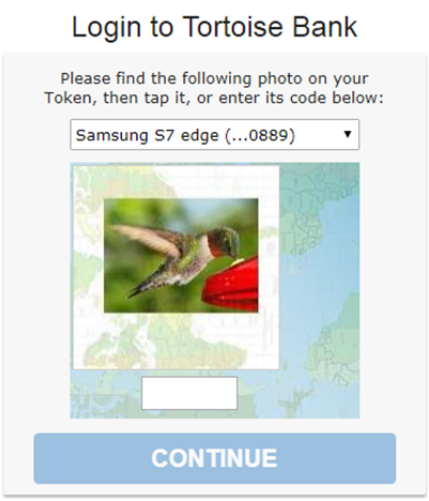
Mutual-authentication solves most banking problems except for injected transactions (such as from malware or sophisticated active MitM). CryptoPhoto solves this with non-repudiable digitally-signed confirmations of the intended transaction acquired over second channel that is out-of-reach of the malware/MitM. This is the only practical way to be sure that an instruction received from a customer is genuine.

- Mutual-authentication establishes legitimacy of both parties for a login (but authentication alone is never suitable for transactions).
- Signing establishes the authenticity and correctness of intended instructions (of any kind, including money transfer, account updates, alias changes, or anything that is important to protect against malicious injections or where the bank requires risk mitigation through single or multi-party non-repudiation.)

- In-device biometrics secure lost/borrowed devices ensuring that only the real customer can approve transactions, and are non-controversial, compliant, and privacy-respectful.

How does CryptoPhoto mutual-authentication work?

CryptoPhoto-protected logins require a user to find and match two identical random photos – similar to the children's card game "snap". This typically takes less than 1 second because humans have an instinctive ability to rapidly recognize matching objects. This matching-step is our clever way to force users to verify website legitimacy during login: they don't need training for this, and do not need to understand how or why it is working. When a photo matches, they tap it to log in. If there is no photo match, it is not your real website, so there is nothing they can tap on to accidentally log in to the fake: they simply cannot be tricked. Our technology prevents imposters stealing both photos and credentials – only your genuine legitimate website is useable by customers to log in to, all fakes are blocked.



Customers do not need to look for browser padlocks, check TLS certificates, or remember and follow other security rules (which nobody does, according to a recent banking study).

Depth and Efficacy of Protection.

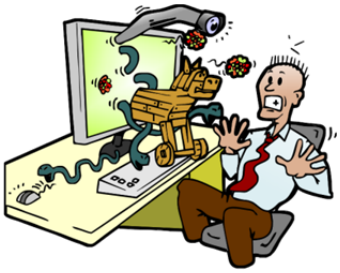
Legacy authentication such as 2FA adds *limited* protection against *some* threats that target *some* user devices, but not the users.

CryptoPhoto's mutual-authentication, signing, and architecture *comprehensively* protect *all* user devices, as well as banking systems and *most importantly*: the actual users themselves.

Key Use Cases.

Block phishing. When customers get fake emails, texts, or other messages, or encounter spoof websites, CryptoPhoto blocks the attackers from stealing credentials.

Prevent Social-Engineering. If the bad guys try to scam your customers with words either over-the-phone, in-person, or online, CryptoPhoto lets your customers know it's a scam, but also prevents them falling prey too.



Neutralize Malware. No matter what evil code has found its way onto your customer devices, CryptoPhoto stops it from injecting fake transactions or performing unwanted actions.

CryptoPhoto works:

❶ online for websites, IoT, and more,
❷ within enterprise and applications,
❸ over the telephone and in call centers for inbound and outbound calls, and
❹ in person (e.g. branches, or in-field relationship managers/advisors/product sales etc).

In all cases, strong mutual-authentication for both parties and reliable digital signatures including non-repudiation with simple, lightning-fast, user experience is provided.

Our next-generation mutual-authentication and transaction-signing solution is built specifically to combat the widest range of modern cyber-security threats, while supporting the fastest and easiest user experience possible.

CryptoPhoto benefits:

- Rapid, high-security user logins and transaction confirmations
- Significant fraud reductions across all channels (online, phone, in-person)
- Reduced call-centre customer-verification burden; cuts call times by 33% on average because customers know the call is genuine, and authenticate in-call in just seconds.
- Reduced social-engineering risks for staff and customers
- Removes customer annoyances, like wrong antifraud rejections and login complication
- Broad protection coverage, including hard "out of scope" problems competitors ignore
- Fast and easy to use, to set up, and to integrate with existing and future systems
- Enables safe 3rd party integrations to banking systems, like FinTech and Identity solutions
- Does not use customer identity, for easy compliance and strong server break-in mitigation
- So fast and easy it's suitable for all transactions: no need for step-up or risky compromises
- Uses mobile phones/tablets (all kinds) or inexpensive physical tokens for the login factor
- Industries lowest TCO, fastest RoI and highest authentication-assurance level: LoA3/AAL3

Features

Fast ✓ Easy ✓ Secure ✓ Self-Service enrolment ✓ Self-service loss-handling ✓ & re-enrolment ✓ iOS ✓ Android ✓ WindowsPhone ✓ Blackberry ✓ phones and tablets ✓ biometrics ✓ signing ✓ works online and offline ✓ privacy supporting ✓ two-man-rule ✓ non-repudiation ✓ mutual authentication ✓ works internationally ✓ 2FA multifactor ✓ keeps working without data connections ✓ no training ✓ also works without phones / tablets ✓ also works in-person ✓ and during phone calls ✓

Threat Coverage

Phishing ✗ Banking Malware ✗ Man-in-the-middle attacks ✗ and Rogue-WiFi ✗ Keyloggers ✗ Site spoofing and impersonation ✗ Social Engineering ✗ (against both customers ✗ and staff ✗) Shoulder Surfing ✗ Unmotivated ✗ or Unsophisticated users ✗ Poor user password practices ✗ Serverside breakins ✗ and Hacking ✗, Dictionary attacks ✗ and customer-lockout denial of service ✗ Harvested/re-used credentials ✗ MitB ✗ User error ✗ Loss/recovery exploitation ✗ CNP fraud ✗ ATM skimming ✗ Telephone scammers ✗ in-person scams ✗

Next Steps:

Our fastest integration to-date into a front-end banking system took just one-week.

CryptoPhoto is written by expert security coders from the banking industry, and is carefully designed for rapid integration with either your web frontend, or your web application firewall (no core or frontend changes necessary). We use a privacy-first, regulation-compliant “separated architecture” to remove risk and speed approval.

Contact: tech@cryptophoto.com

Q: Which is more important? Security, or, User-Experience ?
A: Really, the answer is both. For without great UX, security gets avoided or not used at all.