Cyber Security Toolkit

central 1

Central 1 & Cyber Security

Ever vigilant

Cyber Security is everyone's concern—yours, your customer's and ours. That's why Central 1 has a multi-faceted and on-going approach to keep all financial data safe and sound.

Cyber attacks are the price we pay for the wonderful freedoms of modern banking. The same electronic avenue we use to click into an amazing array of banking services is the same road hackers use to try to break into banks.

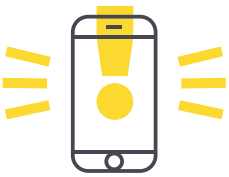
We don't make it easy for them. Central 1 does everything possible to make life hard for hackers and keep criminals out. And there's some things you can do too.

Stringent policies and procedures at the banking system level are good but the job isn't done until you train employees and educate customers on how to stay safe online—even when they're not banking. That's how vigilance is done right.

A growing concern

In a world where attacks grow by more than 30% a year, it's good to know Central 1 monitors every relevant transaction for suspicious activity.

Canadians are a huge target



In 2019 39% of all phishing attempts globally occurred in Canada, with the USA only at 6%.

RSA Quarterly Fraud Report. (2019), 2(2)

Top Phishing Target Countries

Canada	39%
Spain	12%
India	11%
Netherlands	7%
South Africa	7%
United States	6%
Phlippines	4%
Poland	2%
Mexico	2%
Turkey	1%

Police and Thieves of the Digital Age

There are no limits to what criminals will do to break into banks—it's always been that way. In the old days, we called them bank robbers. Today, they're called hackers. Here are some of the current threats you should be aware of.

THREAT & RESPONSE

Brute force

This is the simplest and most reliable form of attack where criminals try endless combos of usernames and passwords until they break in. Their computers can run enough passwords—even 8-character alphanumeric ones—that they can decrypt a weakly encrypted system in as little as 3 months.

Defend yourself against brute force attacks

- **Increase password length**
- **Increase password complexity**
- **Limit login attempts**
- **Implement reCAPTCHA**
- **Implement Botnet Protection**

Phishing

Phishing exploits your customer's good nature and sense of trust by duping people into opening an email, instant message or text message from a fraudulent sender. When your customer downloads the link, malware is installed on their computer or phone or they are taken to a fraudulent website.

Not lacking in audacity, criminals will even "borrow" the look and feel of your website to steal customer login credentials and commit fraud. Your business is then exposed to a host of losses aside from financial, including loss of trust and possibly even declining market share.

Defend yourself against phishing attacks

- **Increased Authentication**
- **RSA FraudAction**
- **Customer education**

Distributed Denial–of-Service (DDoS)

When you hear about a company's website going down, it's generally because of a DDoS attack. By overwhelming a server or network with more traffic than it can handle, hackers are able to bring it down and steal the data they want. Attacks are done through a network of remotely controlled computers known as bots.

We defend you against DDoS attacks

- **Botnet**
- **Silverline (*MemberDirect*®)**
- **Hybrid Signaling**
  - **Real-time Cloud-scrubbing**
  - **DNS traffic protection**
  - **Protocol anomaly detection**
  - **L3-L4 DDoS protection**
  - **L7 DDoS protection**
  - **Amazon Advanced Shield (Forge)**

In the first half of 2019, fraud attacks increased 80% from financial malware

Malware

There are many types of malware including viruses, ransomware, spyware, worms, Trojans, and just about any other type of software hackers can write to gain unauthorized access to a computer system or network.

Defend yourself against malware attacks

- **RSA FraudAction**
- **Teach customers about the importance of keeping their systems updated and having antivirus / malware protection.**

Man-in-the-middle (MITM)

Hackers can also interrupt what you might consider a private communication by eavesdropping or inserting themselves right into the middle of it. Financial sites are especially susceptible to MITM attacks between login and authentication. Criminals can intercept, send and receive data never meant for them and the victim doesn't realize it until it's too late.

Defend customers against MITM attacks

- **Robust encryption and data authentication**
- **Use of certificates**
- **Better SSL/TLS configuration**
- **Compliance with HTTP Strict Transport Security policies**

Don't forget to teach your customers to

- **Avoid banking on unprotected wifi & public networks**
- **Delete cookies**
- **Log out after they are done banking**

Social Engineering

As simple as an old con trick, social engineering manipulates people into divulging confidential information to a person who they think is trustworthy. A fraudster can phone a customer pretending to be a bank officer, or even call another bank officer in an attempt to obtain sensitive customer information. This is often one of many steps in a more complex fraud.

Defend yourself against social engineering

- **Employee and customer education**

Keystroke Logging

Keystroke logging happens when hackers stealthily capture the actual keystrokes on a keyboard while the user is caught completely unaware. Data like usernames and passwords can then be retrieved and used for nefarious purposes.

Defend customers against keystroke logging

- **Teach customers about the importance of keeping their systems updated and having antivirus / malware protection.**

4 Tips For Customer Education

Tip 1: Check that URL addresses correctly match the company you are dealing with and beware of those that have unexpected dashes or numbers in them.

Tip 2: Don't open files from sources you are unfamiliar with. If it doesn't feel right, go with your gut.

Tip 3: Enhance the security of your computer with a good antivirus software to block these types of attacks

Tip 4: Always make sure you have the most recent operating system and web browsers downloaded to your device.

LAYERS OF DEFENSE

When it comes to your customer data, Central 1 leaves nothing to chance.

Our platforms are built on top of multiple defense layers that mitigate cyber threats, both during development and production, while providing key benefits to customers.

INTERNAL

Authentication	Increased Authentication	Enhanced PAC	Weak PAC Detection	Umpire/PAC Blocker	ID Verification
Malicious Activity Detection	reCAPTCHA	Risk Engine Case Manager	Member Alerts	RSA FraudAction	Security Information & Event Management (SIEM)
Application Security	Secure Development	Penetration Testing	Static Code Analysis	Security Training	Independent Reviews
Network Security	Botnet Protection	Silverline DDos Protection	Intrusion Prevention System (IPS)	Transportation Layer Security (TLS) 1.2	
Platform Security	Disaster Recovery	Data Encryption	Server Hardening	Vulnerability & Patch Management	Physical Security
Operational Security	24/7 Threat Monitoring	Security Incident Management	Problem Management	Security Education & Webinars	

Authentication

Authentication is the very first step in protecting customer data. It's how we identify customers by username and password and bar attempts at fraudulent logins.

Enhanced PAC

This allows Central 1 clients to move their customers from numeric to alphanumeric PAC configurations and create longer PACs up to 30 characters. This significantly increases the number of PAC combinations and decreases the possibility of accurately guessing a customer's PAC through brute force attacks.

Weak PAC Detection

Now when customers change their PACs, the strength of their chosen password is displayed in real-time, prompting them to create stronger ones. PAC strength is determined by the estimated number of guesses required to replicate it. Weak PACs (e.g. 1234567) will be rejected by the system for new customers, and existing customers can be prompted to update to a stronger PAC at their next login. It can also protect customers with weak PAC by not allowing login during times of increased threat.

Increased Authentication

Increased Authentication delivers an additional layer of security via 2-Step Verification or challenge questions. 2-Step Verification uses a one-time password sent through SMS or email, where challenge questions and answers are set up by the customer. When Risk Engine determines a suspicious interaction, the user is prompted to enter their password or answer one of their challenge questions.

How does a customer register for Increased Authentication?

Once Increased Authentication is in place, your customers will be prompted to sign up for 2-Step Verification by registering an email or SMS enabled phone number to receive a one-time password when the Risk Engine detects suspicious login activity. Alternatively you can enable your customers to register challenge questions to step up their authentication. These questions are presented only when the Risk Engine is triggered.

How does a customer log in to their online banking with Increased Authentication?

Customers log in to online banking normally. Risk Engine works invisibly in the background so that only suspicious activity is challenged by entering a one-time password or one of the challenge questions to let the system know the login has been authenticated and can proceed normally.

What happens when a customer enters their one-time password or challenge question answers incorrectly?

Customers will be given 3 attempts to answer the question correctly. If their inputs are incorrect 3 times they will be locked out of online banking and will need to contact your financial institution to unlock the account.

Umpire

Ever since MemberDirect began, Umpire has been protecting your data in the background. It's a first line of defense against fraudulent login attempts and brute force attacks that blocks login access when unusual attempts are detected.

What is the advantage of setting up Umpire with Central 1 over my banking host?

Umpire offers PAC Blocker, which has proven to be valuable in fending off brute force attacks. If you choose to implement Alerts, setting up Umpire with Central 1 also allows you to send instant/real-time alerts to your customers whenever the account gets locked.

PAC Blocker

Automate blocking logins when spikes in suspicious activity are detected. PAC Blocker counts the number of failed logins on individual PACs. If the count reaches 50 in a single day, then no further logins using that PAC for the affected financial institution are permitted until midnight of the calendar day, at which time the counter resets. This provides protection against brute force attacks that attempt to use the same PAC against multiple accounts.

ID Verification

Secure identification verification, provided in partnership with TransUnion, is triggered when a user wants to enroll in digital banking, or has forgotten either their PAC or the answers to their challenge questions. Upon successful ID verification, users can update their login information without needing to contact your staff.

Malicious Activity Detection

Malicious Activity Detection is a deep dive into who and what is attempting to get into the system. IDS software regularly scans for unusual activity and alerts us as well as customers.

reCAPTCHA

Hackers like to use 'bots' to attempt multiple, simultaneous attacks on banking sites. It's an easy way for them to test a high volume of accounts with little effort. Owned and operated by Google, reCAPTCHA gets in the way of bots by asking visitors to recognize images, a task that's simple for humans but difficult for bots.

Is there a way to make my computer a trusted device so once you go through reCAPTCHA it doesn't appear again?

No, Google won't allow your computer to become a trusted device. It would make it too easy for fraudsters to bypass the reCAPTCHA tool.

Risk Engine & Case Manager

Working seamlessly with Increased Authentication, Risk Engine & Case Manager use an advanced Bayesian algorithm to detect suspicious activity. Establishing typical customer usage patterns by device, location and other habits makes it easier for fraudulent behaviors to stand out.

Once a suspicious transaction is spotted, Case Manager automatically notifies your institution. Depending on specific rules, Increased Authentication can require your customers to step up authentication via 2-Step Verification or by answering challenge questions. You can set your own policies for when users should be required to step up their authentication, and when a case should be created for investigation by your fraud analysts.

How does Risk Engine & Case Manager work?

Risk Engine creates profiles for each customer that includes device, location and a series of behavioral patterns. Risk Engine automatically evaluates and scores every customer transaction against this profile, assigning a score between zero to 1000, where a score of zero is least suspicious, and 1000 is the most.

Suspicious transactions can automatically trigger additional authentication steps to verify the user's identity, or are forwarded to Case Manager for review by your fraud prevention team.

Alerts

Central 1 gives your customers peace of mind with automated Alerts for all bank accounts. Alerts can be delivered via text message (SMS), email and in-app push notifications to protect a wide range of account conditions:

Security Alerts
account activity such as the addition of a new bill payment vendor, or if their Personal Access Code has changed

Balance Alerts
for insufficient funds or an account balance that drops below a pre-set minimum

Transaction Alerts
when pre-set limits are exceeded on deposits or withdrawals, and when a bill payment may fail

Small Business Alerts
for signers of pending approvals and transactions near expiry (Small Business accounts only)

RSA® FraudAction

RSA FraudAction protects your business from the latest online and mobile threats. It's a third-party service that proactively identifies and prevents phishing, Trojan attacks, and mobile rogue apps by providing real-time alerts and forensics as well as site blocking and shutdown.

Security Incident Event Monitoring platform (SIEM)

Central 1 uses some of the best intrusion detection and prevention software to detect, block and automatically respond to potential threats. Details of these events are logged and sent to the SIEM for analysis.

Network Security

Botnet Protection

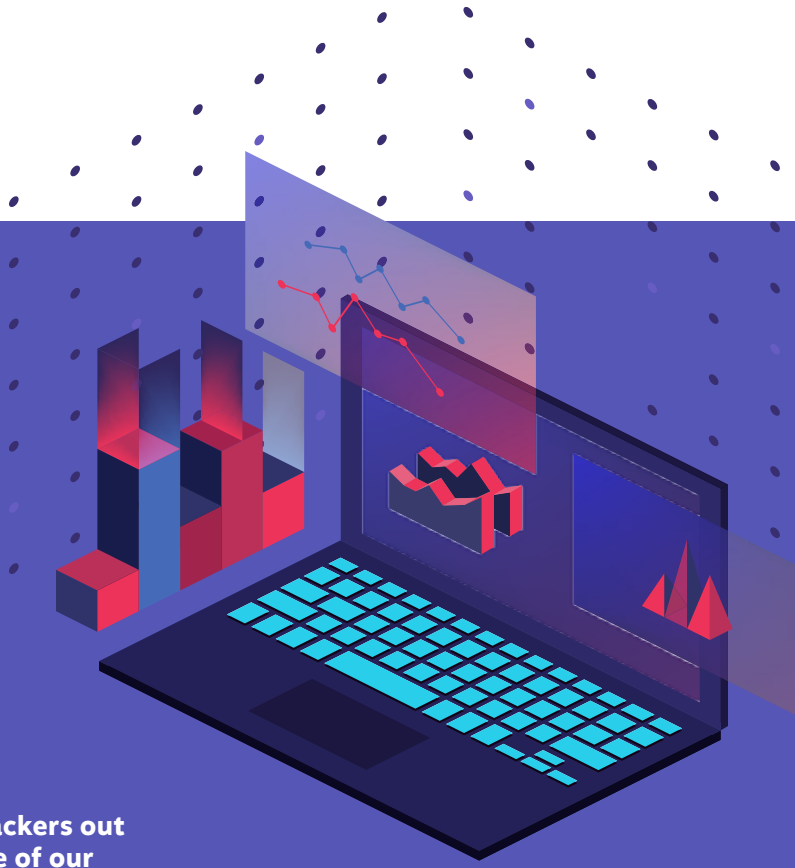
Botnet Protection service analyzes login traffic and prevents automated brute force attacks from reaching their intended destination, your banking host. The platform operates in the cloud and is completely transparent to customers as they bank online. It uses a small JavaScript “token” which analyzes customer behavior.

Malicious behaviors blocked by Botnet Protection:

- Modification or removal of the token
- High volume of login requests from a single IP address
- Users that click in exactly the same area of the screen or press the keys with the exact same timing each time they attempt to login

Prevention is the best strategy

Criminals learn quickly where security is strongest and move on to areas that are weaker. That’s why we’re continually probing for weaknesses in our own systems and protocols.



There’s more than this.
But some things are better kept between us.

You can’t be too careful when it comes to keeping hackers out of financial data. That’s why you’re only seeing some of our authentication and detection architecture here in this toolkit.

Get your Forge Cyber Security Whitepaper to get the complete picture and learn more about our Application, Network and Platform Security layers. Ask for your Relationship Manager for a copy.

Implementation Cost & Effort

Protection Layer	Feature	Implementation Costs	Operating Costs	Banking Host Development
Authentication	Strong PAC	Yes	No	Yes
	Extended PAC	Yes	No	Yes
	Weak PAC Detection	Yes	No	No
	Increased Authentication	Yes	Yes	Yes
	Umpire	No	No	Yes
	ID Verification	Yes	Yes (TransUnion)	Yes
Malicious Activity Detection	reCAPTCHA	No	No	No
	Risk Engine/Case Manager	Yes	Yes	No
	Alerts	Yes	Yes (SMS)	Push/Pull Alerts - Yes Direct Alerts – No
	RSA FraudAction	No	Yes	No
	Intrusion Protection and Prevention	No	No	No
Network Security	Botnet Protection	Yes	Yes	No

BEST PRACTICES

Be a part of the solution

Central 1: Built-in Cyber Security you can bank on

When it comes to protecting customer data and your bank's reputation, Central 1 works behind the scenes protecting data and watching every customer transaction. Here's what you, your employees and your customers can do to help.

Policies & Procedures

- Only set up online accounts for customers who have given explicit consent
- Review 'inactive' online accounts and disable if required
- Enforce strong PAC policies that can stand up to Brute Force Attacks

Customer Education

- Help customers recognize phishing
- Encourage customers to adopt strong passwords and have them change them more often
- Recommend customers sign up for Alerts
- Keep software up to date

Implementation

- Set up a '3 strikes and you're out' policy that locks out users after 3 failed attempts (Umpire & PAC Blocker)
- Implement increased Authentication with Risk Engine & Case Manager
- Use RSA FraudAction or a similar service that monitors for phishing sites, Trojan attacks and rogue mobile apps
- Use reCAPTCHA or Botnet Protection on login pages to prevent bot attacks
- Set up Alerts to inform customers of unusual account activity

Get Busy

Employees and customers need to realize hackers are always out there, trying to break in. It's a proven fact that awareness of hacking tactics diminishes rates of attack. It all comes down to education and training.

Ask yourself:

- How are we currently handling cyber fraud?
- Are we using Risk Engine?
- What resources and policies do we have in place to handle cyber crime and do we need more?
- How good are our password practices?
- How do we push customers to change and use strong passwords?
- Do we have a policy of contacting Central 1 when there is an attempt or a breach?
- Does Central 1 know who to communicate with on our team should an attempt occur?

Never hesitate to escalate reports up the chain, nor hesitate to contact third parties like Central 1. We want to know.

What customers can do?

No Cyber Security program is complete without the awareness and participation of your customers. Make sure you tell customers what they can do to keep hackers out of their personal computers and mobile devices.

Tell them:

- The difference between strong and weak passwords
- Not to use birthdays or other easily guessable combinations like house or apartment numbers
- Not to set security questions for *Interac* e-Transfers® that are easy to guess.
- To update their device's software as soon as updates are available
- That Alerts will let them know when unauthorized activity is spotted on their accounts
- To think before clicking on a link, even from a sender they know

It takes a great deal of spending, staffing, and infrastructure to stay on top of Cyber Security threats—something Central 1 has always done and will continue to do for your business.

- To recognize fraudulent websites that mimic your brand
- To know what you will and won't ask them by email, text or phone

What's in it for you/them

What's in it for you?

- Protection against fraud losses and reputational damage.
- Prevents system outages that result in lost revenue from lost transactions.
- Improves customer confidence that you can help protect them against cyber security attacks.
- Better data as customers become willing to share more personal information with you as their trust grows

What's in it for your customers?

- **Protection**
  their finances and personal information are safe with you.
- **Peace of mind**
  you're protecting them from privacy and cyber security breaches
- **Control**
  customers feel like they have control over their personal information
- **Awareness**
  the better informed your customers are the better decisions they can make to protect themselves

More Information
Contact your Central 1 Relationship Manager at: relationshipmanagement@central1.com

Order Today
To get started today, place your request with Service Now.

Support
Support@central1.com
T 1 888 889 7878

central 1
central1.com