Safeguard Yourself From AI Chatbot Scams

Artificial intelligence (AI) chatbots offer round-the-clock assistance. They can answer questions, reduce wait times, process transactions, and guide you through complex websites or enrollment processes.

With the release of conversational large language models like ChatGPT and Bard, chatbots have become more humanlike in their inferences and responses. Unfortunately, advancing AI has also increased scams like phishing and deepfakes. AI can be trained for good or bad things — and you can count on criminals to train theirs to scheme.

HOW CHATBOTS EXPLOIT HUMANS

Scammers have learned to exploit your trust in chatbots by creating malicious versions or taking over legitimate ones. One method cybercriminals use is phishing. It's a fallback because it works. Whether AI or human-driven, phishing ploys share the same elements:

- They scare or provoke you.
- They create a time-sensitive crisis or offer.
- They provide an immediate, one-time solution.
- They continue to play on your emotions to build fear or trust.
- They pressure you to act without thinking.
- If you question their methods, they bully or manipulate you.

Scams use convincing stories that seem plausible when you're too afraid or excited to question the details in the moment. But the story falls apart when you stop to think about it. That's why fraudsters don't give you time to think about what's happening or ask questions. Chatbot scams are no different, but they might be able to deliver a more convincing con.

Here's an example of a chatbot hoax to give you a taste of how they operate.

A CHATBOT BANK STING EXAMPLE

Take Sara, a LocalBank customer. When she banks online, she uses the bank's AI-powered chatbot. One evening, she gets an email from LocalBank about suspicious activity on her account. The email directs her to click a link to verify the transaction. Sara assumes the email is safe and clicks the link.

But the email isn't safe. It's a phishing email designed to look identical to LocalBank's emails. The email is convincing except for a misspelled bank website in the "from" line and a corrupt link embedded in the "verify" button. But Sara overlooks the red flags because she is too focused on taking immediate action. She fears her bank account is in jeopardy.

Instead of protecting her from a hacker, the email leads Sara directly to one. The "verify" link redirects her to an imposter chatbot identical to LocalBank's, ready to take her information. The chatbot asks her to enter her account number and password to verify and stop the suspicious transaction. Then, the chatbot asks for a verification code sent to her phone, making it sound like it sent the code.

- **What Sara thought happened:** Her LocalBank team stopped a fraudulent transaction using a secret code. Her money is safe.
- **What actually happened:** The hackers used the account information and one-time password (OTP) she gave them to verify her identity for LocalBank. This allowed the criminals to circumvent the two-step verification process from LocalBank and drain her account.

To make matters worse, Sara's bank won't compensate her for the loss. That's because she willingly gave the hackers access to her account, even though it was a hoax.

Sara's experience is common but preventable. Now that you know some of the tricks, learn how to stay cool and protect yourself.

TIPS TO AVOID A BANKING CHATBOT STING

Never allow anyone to scare you into giving information or acting right away. Banks don't send unexpected attachments or ask you to reply with sensitive account information. And they will never ask you to tell them your authentication codes.

If you receive an email stating it's from your bank, take a breath and review the entire email. Is the domain name misspelled? Use your mouse to hover over embedded links and buttons without clicking on them. If a link seems odd, don't click on it. Instead, go to the bank's official website and log in from there.

If you receive an unexpected call from your bank, hang up and don't respond.

Don't use contact information or links in the email, or the callback number displayed on your caller ID. Instead, call your bank using the contact information on your bank-issued credit or debit card. Explain the situation. They'll tell you if it's a scheme. Your report will also help other customers avoid fraud.

Fraud victims often recount feelings that something "wasn't right," but they dismiss their instincts. Go with your gut feeling, and don't worry about upsetting anyone. If you hang up on a legitimate bank, they won't be angry for your vigilance. Banks want you to be safe because they also lose when customers get defrauded.

PROTECT YOURSELF FROM GENERAL CHATBOT SCAMS

Safeguard your information with these tips:

- Access business chatbots through official platforms and websites.
- Be cautious about clicking on links you receive through emails, texts or social media, even if they appear to be from familiar companies. AI-enabled fraudsters use targeted marketing scams to enter people's feeds. They can even use direct messaging apps to entice potential victims.
- Never share your OTP, account passwords, social insurance number, medical account information or any other sensitive data, even if the chatbot asks.
- Connect with businesses directly using their official websites or toll-free numbers, especially for transaction disputes or discrepancies.
- Be wary of chatbots offering outrageous deals and demanding immediate action or sensitive details to claim them. If it seems too good to be true, it probably is.
- Pay attention to how they're treating you. Legitimate companies don't need your personal information to transact business, and they won't get angry with you if you question them. If someone pressures, bullies or threatens you, hang up. Report the incident to local authorities.
- Canada revenue and provincial agency scammers use AI to scare people. They might threaten to cut off your benefits or demand repayment over the phone. Don't disclose any information. If you suspect you're being scammed, hang up. Call the main number instead.

Chatbots have introduced a new level of convenience to our everyday lives, but they come with risks. Be cautious and trust your senses. If it seems suspicious, disconnect. Stay cybersafe out there!

If you have questions specific to your business, or would like additional information, please reach out to your HK Henderson Advisor.

LET US HELP YOU MANAGE YOUR RISK

Saskatoon
Regina
Moose Jaw

hkhenderson.ca
info@hkhenderson.ca
1.888.661.5959