Video transcript: How to Protect Yourself from Malware

Note: Ominous music plays.

[Voice-over] One of the most dangerous fraud threats targeting businesses today is called malware.

On screen: A line icon of a bug grows in the center of the frame, surrounded by circles and binary numbers. A computer monitor animates in and the bug snaps onto the center of the monitor's screen.

[Voice-over] Malware is malicious software designed to gain access to your computer without your knowledge.

On screen: More bugs begin to appear from the bottom of the monitor's screen. The bugs crawl up and disappear into the top of the monitor.

[Voice-over] There are many kinds of malware, such as viruses, spyware, worms, and Trojans.

On screen: A window pops up on the monitor with a white skull and crossbones icon on an orange background. Dashed lines come out from the malware window with icons representing virus, spyware, worm and trojan.

[Voice-over] The malicious program is introduced through a link, attachment or image in an email or website.

On screen: Three circles appear in the middle of the frame. The first is filled with a wireframe globe icon representing a link. The second is filled with a paperclip icon representing an attachment. The third is filled with a photograph icon representing an image in an email.

[Voice-over] It may be disguised as an enticing prize offer or a document marked "important" to get you to act.

On screen: A large computer monitor enters the frame. An email pops up with the subject line, "Congratulations! You've won!!!" The body of the email reads, "Dear Sam, Congratulations! You've won! Claim your prize below!" A large button displays, "Click here to claim your prize!" The email is signed, "Sincerely, Joe Adams, Grand Prize Administrator." The subject line pops out for emphasis and the word IMPORTANT is added to the front of the subject.

[Voice-over] With just a click, the malware quickly enters your company's network and spreads like a disease.

On screen: A cursor clicks the button in the email to claim the prize. The monitor's screen turns orange with the skull and crossbones icon in the center. The monitor with malware window shifts to the left to make room for four smaller monitors representing other computers in the network. Dashed white lines travel from the original monitor to each of the smaller monitors, and a malware window with skull and crossbones pops onto each screen.

[Voice-over] Fraudsters gain access to user IDs, passwords, account numbers and other private data.

On screen: Three circles appear in the center of the frame, each with a fishing hook hanging above. The first circle has a user ID icon. When the audio says "user IDs," the fishing hook above comes down and grabs the user id circle and pulls it up and out of the frame. The second circle has a password icon. When the audio says "password," the fishing hook above comes down and grabs the password circle and pulls it up. The third circle has a Regions Visa credit card icon. When the audio says "account numbers," the credit card circle gets hooked and pulled up off screen.

[Voice-over] They may take over or monitor computer activity, change payment instructions, initiate financial transactions, or delete critical files.

On screen: A computer monitor appears with an online banking personal checking account page on screen. A transparent gray overlay covers the account page while a spotlight highlights the available balance and account number. The Transfers tab in the page navigation is selected, and the Transfer To account is modified from a Savings account to the Fraudster's account. Transfer Money button is selected. A window appears with folders labeled Banking records, Compliance documents and Customer data. All three folders are highlighted and dragged into the computer's trash can.

[Voice-over] Warning signs of malware infection include unfamiliar login screens, pop-up messages or slow-running applications.

On screen: A login window appears on the computer monitor, followed by a pop-up message with a large alert icon. Finally, a window with a loading indicator displays.

[Voice-over] Most malware infections happen through risky human behavior on a computer or mobile device and can be avoided.

On screen: The computer monitor now has a dark background with a white bug icon on it. The monitor shifts left to make room for a mobile device with the same dark background and white bug. Red circles with a white x in the center appear over both devices.

[Voice-over] You have the power to help prevent this vicious attack.

On screen: The background of the video transitions to white and a filled dark blue circle fills the center of the frame. A shield icon animates in the center of the circle.

[Voice-over] Make sure your antivirus and firewall programs and recommended patches are up to date.

On screen: The filled dark blue circle shifts right, and a filled green circle of the same size animates in on the left. A magnifying-glass-around-a-bug icon animates in on the green circle. A fire-and-brick-wall icon animates in on the blue circle.

[Voice-over] Set up firewall parameters to prevent employees from visiting high-risk websites.

On screen: The two circles merge into the center with the blue circle and firewall icon on top. The green circle disappears behind the blue circle.

[Voice-over] Add warning banners to clearly identify emails received from outside sources.

On screen: The blue circle animates off screen revealing the green circle underneath. An envelope-with-alert icon animates in on the green circle.

[Voice-over] Never open an email attachment or link from an unknown sender.

On screen: The green circle shifts left and the blue circle animates in on the right. A red circle with a white x appears in the bottom center, overlapping both circles. A paperclip icon animates in on the green circle. A wireframe globe icon animates in on the blue circle.

[Voice-over] Report and delete suspicious emails immediately.

On screen: The red circle with white x disappears. The icon in the green circle morphs into a megaphone with sound lines, and the icon in the blue circle morphs into a circle with an x in the center.

[Voice-over] Think twice before clicking on links, photos, offers or advertisements online.

On screen: The two circles move to stack vertically, with the green circle on top with a wireframe globe icon in its center, and the blue circle on the bottom with a target and bullseye icon in its center.

[Voice-over] Hover over links to confirm the URL or web address.

On screen: The top green circle with wireframe globe transitions to the center of the frame while the blue circle disappears behind it. The audio text, “Hover over

links to confirm the URL or web address," appears in grey underneath the green circle. A cursor appears and hovers over the text, changing the text color to blue and adding an underline. A grey box appears below, displaying the representational-only url: http://www.confirmthewebaddress.com.

[Voice-over] Create internal controls to validate any changes in payments or payment instructions.

On screen: The green circle animates off screen revealing the blue circle. A checkmark icon animates inside the blue circle.

[Voice-over] Provide ongoing associate training on fraud threats and your internal processes for handling.

On screen: The circles stack vertically again, with a fraudster icon in the top green circle and a spinning gear icon in the bottom blue circle.

[Voice-over] Empower your team to fight against malware attacks and keep your business safe: you'll be glad you did.

On screen: A filled blue unlocked lock appears in the center of the frame. Bugs crawl up on the lock, trying to get inside. The screen fades to white and the words, "You'll be glad you did," animate in grey on the center of the screen.

[Voice-over] For more fraud prevention tips, visit us at www.regions.com/stopfraud.

On screen: Scene fades to white and the Regions logo animates in.

Disclaimer appears under the logo: The information presented is general in nature. Regions reminds its customers that they should be vigilant about fraud and security and that they are responsible for taking action to protect their computer systems. Fraud prevention requires a continuous review of your policies and practices, as the threat evolves daily. There is no guarantee that all fraudulent transactions will be prevented or that related financial losses will not occur. Visit regions.com/stopfraud, or speak with your Treasury Management Officer for further information on how you can help prevent fraud.