Protecting Your Financial Identity

A man with dark glasses and a black hat appears on the left side of the screen. A list titled Wanted for Cybercrimes appears on the right. The list includes email fraud, identity theft, stolen data, phishing scams, network intrusion, and malware. **Narrator:** "Meet Hal. He's a cyber-hacker, out to steal your identity, and he's come up with a lot of different ways to go about it."

Hal sits down at a computer and starts typing. Different lines of hypothetical code stream across the background, representing his input. **Narrator:** "Once he has the information he needs, Hal might withdraw money from your bank account, set up new credit accounts to make expensive purchases, get health services using your name or insurance, or sell your personal information to someone else."

A different man appears in a living room. Dozens of sheets that say Final Notice, Past Due, and Account Suspended drift down from above, until he is half buried in them. A person wearing a suit and carrying a briefcase enters from the right. **Narrator:** "Hal could rack up thousands of dollars of debt before you even realize your identity has been stolen. And it could take years to untangle the mess. It could even cost you money if you have to hire a lawyer or other professional to help you."

Hal is typing at a computer again. This time, the computer screen text indicates that Hal is transferring funds from a bank account. **Narrator:** "Hal is clever. Watch out! He'll use one of his many tricks to try to get you to give up your information."

Hal leans against a computer monitor and the word Phishing appears. **Narrator:** "Phishing is the collection of personal information through an unsolicited email. Here's how it works."

Hal disappears and a pop-up box representing an email appears on the computer screen. The message says Dear valued customer please read this at once. Another box appears, representing a fake website. Then Hal appears typing at a computer again, with information streaming out of the fake website to his computer. **Narrator:** "You get an email containing a link that appears to be from your financial institution or other business. When you follow the link, Hal sends you to a fake website that looks like the real deal. But it's actually set up to capture any personal information you enter."

Hal leans against a smartphone and the words Smishing and Vishing appear. **Narrator:** "Smishing and vishing are similar to phishing. But instead of an email, you get an unsolicited text or voicemail message."

Hal disappears and different icons appear to the left of the phone, representing the narrator's example. **Narrator:** "For example, you might receive a text or voicemail message informing you of a problem with your bank or credit card account. When you respond, Hal gets the information he needs to steal from your account or charge purchases on your card."

Hal stands next to a computer monitor again. As the words Fight Back appear on screen, he hops up and down. **Narrator:** "You don't have to take what Hal is dishing out. There are many things you can do to fight back."

Two smartphones appear on the screen, one with a password login screen, the other with a thumbprint login. The words Complex Password and Fingerprint Scan appear on the sides. **Narrator:** "Use a complex password or fingerprint scan to access your phone to protect yourself if your phone is lost or stolen."

A laptop and a tablet showing a personal identification number appear with a plus sign between them, illustrating two-step verification. **Narrator:** "Enable two-step verification -- an additional layer of security beyond your password -- to safeguard your email and online accounts."

A tablet appears displaying a mobile banking app that is uploading. **Narrator:** "For extra security, install and use your financial institution's mobile banking app instead of going to their website. And don't forget to create a unique and complex password for access."

The camera zooms in on a Remember Me button on a login screen. A red circle and diagonal line are drawn over the button. The user presses a Disconnect button next to the words Public Wi-Fi in the device's settings. **Narrator:** "Always say "no" to automatic logins. And never use public Wi-Fi to access your financial accounts."

The screen shows personal details on a computer screen. A red circle and diagonal line are drawn over the information. **Narrator:** "Avoid sharing personal details with the public on social networking sites."

An account statement appears on the screen. The statement contains a suspicious transaction, and a caution symbol appears next to it. **Narrator:** "Review credit card and bank statements regularly for any transactions you didn't make."

The screen shows a Credit History report, then zooms in on a suspicious transaction, and a caution symbol appears next to it. **Narrator:** "Monitor your credit reports to spot accounts you didn't open."

The scene changes to a person sitting at a desk typing on a computer. **Narrator:** "You can request free reports at annualcreditreport.com."

Hal is back on his computer, trying to scam users. **Narrator:** "Identity thieves like Hal are constantly looking for new ways to commit fraud. Be proactive about protecting your information."

The final screen appears, which reads, It's your future. Start planning today.