SEXTORTION SCAMS

BY JAY BORDEN

Sextortion scams aren't new. They've been around for years. Older versions simply sent an email saying they had pictures of you doing things you wouldn't want publicized. We won't go into any more detail here.

The current version of this scam still arrives as an email. But it goes further by addressing you by name. It talks about how they installed spyware on your computer and have been watching everything you do and every site you visit. They go so far as to name the software installed. Whether it is real or not doesn't matter as most people will have no idea about that.

The cybercriminals claim the software they installed allowed them to compromise your computer and its webcam. This let them watch and record you doing these private things you wouldn't want publicized and record all the websites you visit. Share the email with anyone and they will send the video to all your contacts. It is made clear they have the ability to do that and will not hesitate to do it.

But this new scam goes even further. The email includes a picture of your street and your house to convince you that what it claims is real. Also included is a threat to come to your house if you don't pay.

Some messages include a password you may have used at some point with your email. This is to prove they have access to your computer.

Of course, a ransom is demanded. Failure to pay will result in the release of the video to all your friends and contacts.

The ransom is supposed to be paid in bitcoin to make it difficult to trace. The ransom in the example cited was a bit under $2000. The payment could be made by scanning a QR code in the message. Scanning the QR code will almost certainly result in malware being downloaded to your device.

SEXTORTION SCAMS

CONTINUED

What to do.
Before you get upset and worried, remember that much of the information they have is very easy to obtain from public sources.

Don't fall for fake threats. Stop and think, is all the information in the email publicly available? If so, then the chances of them having private information isn't high. It is possible, but then anything is possible.

If the letter or email contains your name, email address, physical address, age, a previous password, and a picture of your street or house, remember that these are not hard to get. Most are available for free. Pictures of your street and house are available on mapping sites and real estate sites. Your name and address and age are available from many companies or can be inferred from other information such as when you graduated from school. The previous password may require more work but is still not hard to acquire. Passwords are for sale on the Dark Web and don't cost much.

Determine if the acts they claim to have recorded or the sites they claim you visited may be true. If not, then nothing to worry about. If it may be true then consider covering the camera in your computer. However, this won't stop someone from listening in on your conversations or tracking sites you visit.

Put better protections on your devices, that will catch these types of malware.

Look carefully at the message. Does it have spelling mistakes, wrong words or other grammatical errors? Anything else that raises a red flag? Then it probably isn't real.

Most of these types of messages are going to be fake with much of the information in these emails publicly available. Mass mailing of spam messages is easy. Remember, cybercriminals don't need very many people to fall for the scam to turn a profit.

Always think before you act.

To learn all the ways we can help make your company and family safer, visit onebrightlycyber.com, contact OneBrightlyCyber at info@onebrightlycyber.com, or call (888) 773-1920.