SCAM REPORT
MILTON TOWNSHIP S.A.L.T. COUNCIL MEETING NOVEMBER 14, 2023

Prepared by Arnold H. Shifrin

Ring™ Video Doorbell Scams

The Ring video doorbell is mounted next to your front or rear door and is used for home security and video surveillance. The doorbell is connected via the internet to apps installed on your devices and allows you to monitor a limited area at the door. The doorbell also permits you to speak to visitors from a remote location. (See attached photograph of a mounted doorbell.)

Scammers believe homes with Ring doorbells may contain valuables that are worth stealing. Thus, these homes are often targeted for burglaries. Scammers have also devised various ploys to obtain personal and financial information from those individuals whose homes have Ring doorbells.

How the Ring doorbell scams work:

- Phishing attacks: Victims receive emails that appear to originate from Ring and are asked to verify their identity and update their account information. The emails may also include malicious links or attachments that, if clicked on, can cause malware infections that place a victim's personal and financial information at risk.
- Fake Ring company representatives: Scammers pose as Ring doorbell representatives selling new doorbells. Homeowners with a Ring doorbell are told their models have security issues or are outdated and should be replaced. The homeowners are asked for their personal and financial information for "software updates" or to purchase new doorbells.
- Fake alarms: Scammers send victims fake notifications stating there is a fire or burglary at their residence to entice them to log into a bogus Ring website and reveal their personal information.

How to protect yourself

- Ring will never contact you and ask for your personal and financial information to "update your account." Any requests for such information originate from scammers.
- If you wish to confirm that an email or text message from Ring is legitimate, contact the company directly. Enter the URL address (www.*ring.com*) in your web browser and click on "Contact Us" at the bottom of the screen. Do not use contact information for the company that was given to you by someone else.
- Do not open attachments or click on links in unsolicited emails from Ring. If you do, you will be taken to a fake website that appears to be legitimate and asked for your personal and financial information. Once scammers have this information, they will attempt to access your Ring doorbell account and view your live video feeds. Your credit card information will be used for unauthorized purchases that are charged to your account.
- If you are notified on your Ring app that there is a fire or burglary at your residence and you are not home, you can confirm if the notice is legitimate by contacting a trusted neighbor or your local police or fire department.
- Ring regularly releases security updates. Be sure the latest software version is installed on your devices and that your web browser, operating system, and antivirus programs are all current.
- If you are a victim of a Ring doorbell scam, change the password to your Ring account and monitor your credit card charges for unauthorized activity. Report the incident to Ring, your local police department, and the Illinois Attorney General Senior Citizens Consumer Fraud Hotline (1-800-243-5377).

[Source: Ring LLC]