# CYBERCRIME: PROTECTING OURSELVES AND OUR FAMILIES ONE CLICK AT A TIME

BY NOAH GIEBEL, NPMHU NATIONAL OFFICE IT MANAGER

The World Wide Web (internet) is a big place and it's growing every minute. And in a world that is becoming increasingly connected through devices such as phones, tablets, and internet connected devices families are exposed to more threats than ever before. A Boston Consulting Group study found that "as many as 98% of children from ages 8–17 are on the internet, and remarkably, nearly three out of four respondents said they had experienced at least one cyber threat".

While using the internet can be a great source of information readily available at the tip of your fingers, it is also a very public information expressway. Knowing how to protect yourself and your family from digital threats is more important now than it ever has been.

NPMHU would like to help you to navigate the world of online threats, so we have put together several tips and tricks (do's and don'ts) as part of a yearly article to help you be better prepared against on-line threats.

## EMAIL AND WEB SECURITY — DO'S & DON'T'S

### DON'T

- Initiate a payment, purchase, money transfer, or any other financial transaction until you've confirmed the payee and related details by phone or in person.
- Click links in emails unless you trust the sender, you've reviewed the link, and you're absolutely sure you know where it goes.

### DO

- Use different email accounts for business, personal and social media.
- Be wary of permuted or spoofed sender addresses (e.g., @nnicrosoft.com instead of @microsoft.com)
- Be wary of request for urgent action (e.g., "your account will be closed," "your account has been compromised," "limited time offer", or "urgent action required"). These types of requests are almost aways SPAM/PHISHING.

## PHYSICAL SECURITY — DO'S AND DON'T'S

### DON'T

- Leave your laptop, cell phone visible in your car or in public.
- Expose passwords in public places such as public transportation.
- Give your devices to strangers.
- Use public Wi-Fi for doing banking or password protected work.
- Leave passwords visible for others to see.
- Leave your home computer or tablet unlocked while unattended.

### DO

- Lock home computer when unused by pressing windows + L.
- Set a password for your devices and when available use biometrics for added protection.
- Question everything
- Ensure you have your home network protected by a password.

## PASSWORD SECURITY

- Make your passwords as long as possible (use a phrase)
- Don't make passwords about you (e.g., don't include your name, DOB, or address)
- Change passwords periodically.
- Use different passwords for different Apps, websites, and devices.
- Enable Multifactor Authentication when applicable.
- **Never share your passwords with anybody**