Dozens of botnets have helped thieves heist more than $100 million from the accounts of businesses around the world. Hackers stole more than $1 million from the payroll accounts of a Washington State hospital. Cyber thieves operating out of Ukraine are believed to be responsible for massive ebanking losses over the past few years.

Cyber criminals are becoming increasingly malicious and sophisticated, using a combination of tactics to gain your trust...and access to your company's financial accounts.

Understanding the tools and methods these fraudsters use can help you protect yourself and your organization.

**Malware** is malicious software installed on your computer without your knowledge or consent. Malware can record your keystrokes, such as your login ID and password when entered online, and send them to a fraudster. Malware can also redirect your browser to a fake site designed to emulate your financial institution's online banking site.

Your computer can become infected with malware when you open infected documents attached to emails, access malicious websites through links contained in emails, or access infected videos or documents on social networking sites.

**Social engineering** is an attempt to manipulate you into performing actions or divulging confidential information by impersonating a trustworthy entity, through email (known as phishing), through text messaging (known as smishing), or over the telephone (known as vishing).

**Denial of Service** attacks, where illegitimate Internet traffic is used to prevent legitimate access to a website, can be used to create distractions to facilitate social engineering attempts, or mask the actions of malware.

**BUILDING A ROBUST DEFENSE**

There is no single action that can completely protect you from cybercrime or attempted cyberfraud. However, a number of actions and precautions, when combined and layered effectively, can provide a robust defense against many major threats.

**Protect your access credentials.** Never provide your User IDs, passwords, token codes, or other similar types of credentials to anyone. If you receive an email, text message, phone call, or other communication purporting to be from your financial institution soliciting sensitive information, or requesting that you take urgent action on a payment transaction, it is likely a phishing or other social engineering attempt.

Do not click on any links or open any attachments contained in these or other suspicious emails. Do not respond, and report the incident to your financial institution immediately.

**Consider using dedicated computers** to access your online banking sites. Limit the sites these computers can access, and consider preventing email access from these computers as well.

**Never access your online banking sites from a WiFi hotspot or from a shared, public computer.**
DON'T LET CYBERCRIME HAPPEN TO YOU

Educate and consistently remind your employees about cyberfraud threats. Even employees who do not have access to your online banking applications can inadvertently spread viruses and malware through your network.

ENGAGE YOUR FINANCIAL INSTITUTION
Your financial institution can be a valuable ally in the fight against cyberfraud. Here are some additional best practices to consider with your bank’s corporate online banking service:

Implement secondary authentication for all funds movement activity. We also strongly recommend using secondary approval for operator maintenance functions — where one system administrator must approve the actions of another system administrator — if the operator has access to any funds movement services.

Keep operator profiles current, with appropriate entitlements and transaction dollar limits commensurate with the employee’s role and your typical transactions. Disable operator IDs for employees out on extended absences, and promptly delete operator profiles for employees who are no longer with your organization.

Take advantage of payments fraud prevention services. For example, PNC offers Positive Pay for checks and ACH Positive Pay for electronic transactions, which should be placed on all of your PNC Bank accounts to prevent unauthorized ACH debit activity.

Use Event Notifications to receive alerts for sensitive types of account and online activity.

Download and install protective software, which may be available through your bank, that can identify and remove malware, help to secure your online banking credentials, and protect against browser hijacking.

Even as headline-grabbing heists are becoming more common — and more costly — you can protect yourself and your enterprise with these common sense precautions.

For more information, contact your Relationship Manager or visit pnc.com/treasury.