CYBERSECURITY GUIDE

F&M BANK

fmbnc.com

Tips to Keep Your Info (and Money!) Safe Online

F&M BANK

fmbnc.com

CYBERSECURITY GUIDE

"Cybersecurity" is everywhere these days. Protecting your data and money from Internet thieves is essential in our high-tech world, but it can feel overwhelming. F&M Bank makes it easier by providing simple guidelines to secure your email, computer, and social media while defending against Ransomware.

Email Safety

Identifying red flags in different parts of an email is the best way to determine whether it's safe to open—or should be deleted ASAP. Everything from the subject line to the hyperlinks offer clues, and your best bet is to become familiar with common warning signs.

Computer Safety

Think about all of the personal and financial information you've entered into your computer. Yikes. Securing your computer is about vigilance, whether it's using complex passwords or ensuring you have an HTTPS connection when paying online.

Social Media Safety

Platforms like Facebook are great for keeping up with long-distance friends and family. But social media can also tempt you to reveal info that cyber thieves can use against you. It's vital to learn what's safe to post and what can make you vulnerable.

Ransomware

Ransomware is exactly what it sounds like: a criminal demanding money in exchange for something you value. In this case, that "something" is data. Your information can be kidnapped (yes, really) when a Ransomware file infects your computer, perhaps when you open a phishing email or visit a deceptive site.

Has your information been compromised?

F&M Bank can help. We offer multiple resources to customers who've experienced cyber fraud.

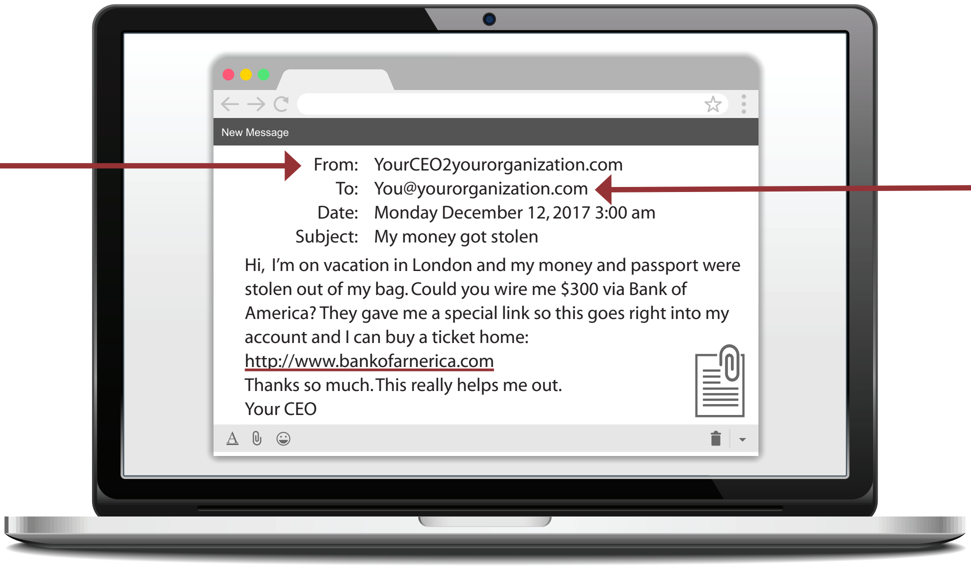
Your cybersecurity is a top priority at F&M Bank. In addition to a comprehensive system of safeguards, we've created easy-to-follow resources that can help you stay safe online.

fmbnc.com/cybersecurity

Email Safety

IS THAT EMAIL SAFE TO OPEN?

It can be tough to tell these days because, often, dangerous emails look legitimate. Identifying red flags in different parts of an email is the best way to determine whether it's safe to open—or should be deleted ASAP. Everything from the subject line to the hyperlinks offer clues, and your best bet is to become familiar with common warning signs.



From: YourCEO2yourorganization.com
To: You@yourorganization.com
Date: Monday December 12, 2017 3:00 am
Subject: My money got stolen

Hi, I'm on vacation in London and my money and passport were stolen out of my bag. Could you wire me $300 via Bank of America? They gave me a special link so this goes right into my account and I can buy a ticket home:
http://www.bankofarnerica.com
Thanks so much. This really helps me out.
Your CEO

Phishing sounds like something nice to do on a warm afternoon. But it's actually an email designed to trick you into revealing personal information (ie: credit card numbers) or get you to click on a link that will do some damage to your computer and/or the financial data on it.

Becoming familiar with common tricks of the phishing trade will help you identify and eliminate risks to your security. Let's get started!

Who is this email from?

The "From" line can tell you a lot about whether you should open an email. Does the address:

- **Look familiar?** Whether from a person or a company, you should recognize the sender. And be sure it's spelled correctly. Some bad guys make their address try to mimic authentic companies' addresses but add, subtract, or change one letter inconspicuously.
- **Come from someone you trust?** If you don't know the sender personally, has someone you know vetted them?
- **Make sense?** The support division of major companies probably aren't emailing you.

Who is this email to?

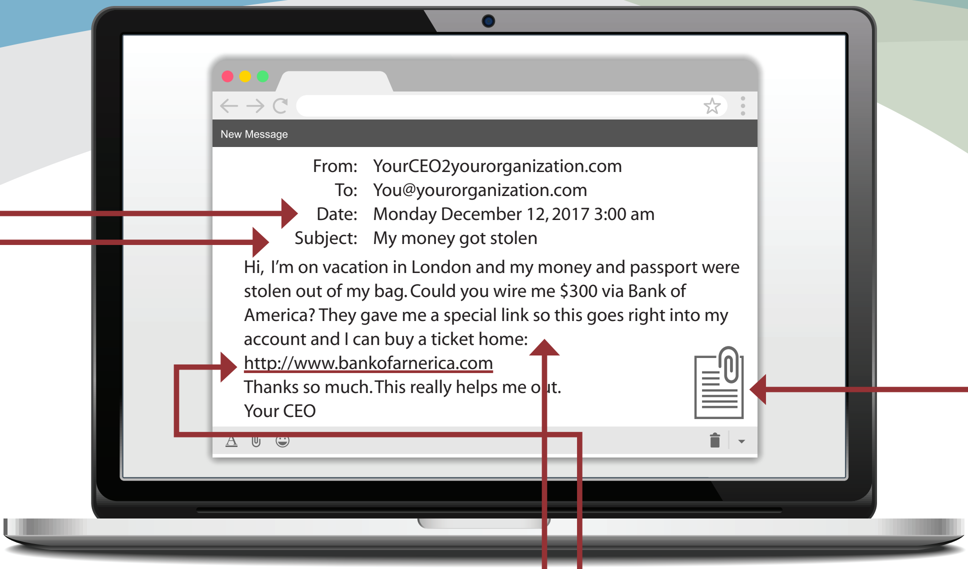
You, right? But a closer look could reveal hints. Is it:

- **Sent to people you don't know?** If you're among a list of people on the "To" line, evaluate whether the group makes sense. You should be able to identify, for example, that the others are in the same division at work or part of your book club.
- **Forwarded?** Be especially vigilant with a chain email. The more hands—or computers—a message has gone though, the more likely it's infected with a bug.

continued

F&M BANK

fmbnc.com



From: YourCEO2yourorganization.com
To: You@yourorganization.com
Date: Monday December 12, 2017 3:00 am
Subject: My money got stolen

Hi, I'm on vacation in London and my money and passport were stolen out of my bag. Could you wire me $300 via Bank of America? They gave me a special link so this goes right into my account and I can buy a ticket home:
http://www.bankofarnerica.com
Thanks so much. This really helps me out.
Your CEO

When was it sent?

The "Date" feature is easy to overlook, but ask yourself:

- **Does it add up?** Maybe your pal is emailing you when you know she's at the movies. But it pays to be suspicious.
- **Was it outside of normal business hours?** Most of the time, business-related emails arrive during business hours.

What's the subject?

The good news is that online con artists often give themselves away by seeking to reel you in in dubious ways. Does the subject:

- **Align with what the email says?** If the subject references a school event for your child but the body content is about low-cost cars, don't click on any links!
- **Provoke a strong emotion?** Inciting fear is a useful tactic for scammers. "I've been arrested!" "I need help!" Many times, it's a setup to get you to send money to alleviate a made-up problem.
- **Reference an email you never sent?** Your doctor is returning an email about an overdue bill. The electric company is responding to your request to pay online. The only problem is that you don't remember sending those emails. When in doubt, call the company—don't give out your financial info.

What's the content?

Here's where things get interesting, so put on your detective hat. Does the email body:

- **Ask me to take a risky action?** Click on this. Send me these account numbers. Pay this "fine" here. They're all red flags.
- **Sound legit?** Your boss' grammar is flawless, so an email from her won't look like it's written by a first grader. Or maybe a message from a friend isn't her style at all.
- **Sound scary or lewd?** Whether it contains a veiled threat ("I know what you're hiding—open the attachment for proof") or a temptation they're hoping you can't resist ("Remember him? You'll never believe what he looks like now!"), steer clear of it.
- **Have the "right" signature?** Generic signatures aren't typical for emails from valid companies; most have details like a contact person, that person's title, and a local or toll-free phone number.

Are there attachments?

Attachments can get you into a world of trouble, so unless you're absolutely sure they're aboveboard, keep your mouse off of them. Is the attachment:

- **Something you were expecting?** If not, make sure the attachment jibes with your life—ie: your child's soccer schedule, snack schedule at church, etc.
- **Contained in a safe file?** Look at the file extension letters to see if you're familiar with it. Text files (.txt) are always okay to open, while .exe are almost always a bad idea.

What about hyperlinks?

Those embedded links that take you to another part of the web should be double- and triple-checked before clicking on them. Is the hyperlink:

- **Flying solo?** Sometimes you'll get an email that's blank except for a hyperlink, which is really tempting for a lot of us. Which is probably why scammers keep them coming.
- **Spelled correctly?** In the same way that a misspelled company name in the "From" line is a problem, a misspelling of a well-known company in a hyperlink indicates trouble.
- **Leading to the right place?** You can see the web address for the hyperlink simply by hovering your mouse over it. If you see any sign that it'll take you to an unfamiliar site, don't click on it.

F&M BANK

fmbnc.com

COMPUTER SAFETY

Don't know where to start when it comes to protecting yourself from information breach and loss? We've made it as easy as possible with this guide to basic computer safety.

Back It Up!

That "uh oh" feeling as your computer takes a last gasping breath? We've all been there. But a computer crash won't lead to complete data loss if you regularly back up the information stored on it. You can use a cloud-based platform or go old school with a thumb drive. Treasured photos, family recipes, business records—it takes just seconds to protect them all.

Get Smart About Passwords

A little sloppiness here can have a huge impact on your personal and professional life. Stay vigilant with these tips:

- **Mix things up.** You know you're not supposed to use the same password everywhere, but many people do. The problem? If a cyberthief figures out your Facebook password, he or she can access every area of your personal, financial, and business life.
- **Change them often.** Not only do you need to create different passwords for different sites, but you need to switch them up often. Many companies require employees to change on-the-job passwords once a month, and it's a good practice at home, too.
- **Get a manager.** A password management tool can be a lifesaver in the modern world. These tools (some of which are free) come up with impossible-to-guess passwords, store them all for you, and then fill them in automatically as needed.

Protect Yourself

Cyber criminals release new versions every day, making them a constant threat to your information. What to do?

- **Load up on software.** Install anti-virus programs that not only safeguard your computer against viruses that are already out there, but the ones that are coming. (Today's technology can read patterns and predict stuff like this.)
- **Go automatic.** Set your software to update on a regular basis so you don't have to add that step to your to-do list.
- **Know your email.** Many viruses find their way inside your computer via emails, so it's worth your time to brush up on how to spot a dangerous email.
- **Watch your plugs.** It's never a good idea to plug someone else's USB stick into your computer.
- **Got HTTPS?** When making an online purchase with your credit card, be sure you're using an HTTPS connection. That "s" is crucial because it means your info is being scrambled.

Kill it With Fire

Firewalls are a must if you ever venture onto the web—and who doesn't? In essence, a firewall stops uninvited info from coming into your computer. Operating systems come with firewalls, but you can double up on security by purchasing a standalone product, too.

Physical Blockers

We often think of bad guys hijacking your data from behind a screen thousands of miles away. But it can happen in the real world, too.

- **Guard your screen.** Using a computer in public locations (think a coffee shop or airport) is incredibly common. Installing a screen guard, a filter that attaches to your monitor, masks what's on your screen unless you're sitting directly in front of it.
- **Lock it up.** If thieves steal your computer, they might be able to access the valuable info on it. Be sure to hide electronics if you must leave them in your car, and use a theft deterrent like a physical or fingerprint lock on your computer.

If you believe your computer has been compromised, F&M Bank may be able to help. We offer multiple resources to customers who've experienced cyber fraud.

Social Media Safety

F&M BANK

fmbnc.com

Social media, which includes personal connection platforms like Facebook and Instagram, as well as professional networking sites such as LinkedIn, are designed for sharing. But thieves can piece together potentially damaging clues about when you'll be away from home, which loved ones or hobbies might make up your passwords, and more. Protecting yourself starts with learning what's harmless and what's not.

Maintain Some Mystery

In the age of (figuratively) baring it all to the world, being discreet feels almost old-fashioned. But it could save you time, trouble, and money.

- **Go vague.** It may seem innocuous, but data like your birthday and where your kids go to school shouldn't be available to the public. Even listing your exact city can lead to vulnerability. Be sure that the outside world has only vague details—listing your "lives in" information as "North Carolina," rather than Salisbury, for example.
- **Keep the past private.** Professional networking sites are designed, in part, to help people explore new job opportunities. And that requires a resume, right? Well, yes and no. Keep your resume ambiguous enough that it can't be used to help an identify thief. Potential (legitimate) employers will be in touch if they're interested in knowing more about your work experience.
- **Be discriminating.** Sure, you'll feel like the most popular kid in class when you have tons of contacts. But the more people you allow into your private life, the higher the odds that something will go wrong. If your circle is already large, ensure that only a trusted few are privy to the really important stuff. Cat videos? Share with everyone. A link to the resort you're visiting next week? Only your best friend gets that info.
- **Shield your location.** When left intact, location services on your phone and other electronic devices can show your exact spot as part of any post you make. Deactivate them to prevent over-sharing.

Know the Rules

A little investigation before you click, hit "post," or agree to accept anything online can prevent damage down the road.

- **Be strict about settings.** Privacy and security settings ensure that only the people you select can see certain posts. The stricter you are (ie: ensuring only "friends" can see your posts, as opposed to strangers or even those marked "acquaintances"), the better.
- **What's the message?** Hackers can try to get into your accounts by posing as a friend via a private message. If you get a message from someone you don't know, ignore it. If you get one that seems strange from someone you DO know, get in touch offline to ensure it's really from him or her.
- **Don't click.** Similarly, be very cautious about clicking on any links embedded in tweets and posts, as that's a prime way for hackers to strike.
- **Avoid endangering your job.** Many employers today monitor employees' social media activity and even have written rules about what actions (think racist or off-color comments) could get you fired. Be aware of company policy.
- **Investigate third-party apps.** You finally download that popular cyber game, but they're asking for access to your account. Before you agree to anything, do your due diligence. Giving access to the wrong third-party app opens up a buffet of info that can be used against you.

Are You Exposing Others?

The details you post and the malware you allow into your computer can hurt not only you, but the people connected to you online. Here's how:

- **Specifics=vulnerability.** Tagging someone in a post about an upcoming event ("Can't wait to see this band in concert with Jane Smith tomorrow night!") broadcasts that neither you nor your friend will be home then. Wait until the event has passed before talking about it online.
- **Copycatting.** Thieves who are able to figure out your patterns and personality can pretend to be you when contacting people in your online circle. A phishing email to your friend that mentions a specific activity you love sounds a lot more authentic than a generic attempt.
- **Log out.** If you use public computers—at the library, perhaps—to access your profiles, make it a habit to double check that you've logged out before leaving the computer. That way, the next person who sits down can't target your friends, lock you out of your own account, or worse.

If you believe your social media account has been compromised, contact the host site for help. If the breach involves financial deception, F&M Bank may be able to help, as we offer multiple resources to customers who've experienced cyber fraud.

Ransomware

The fundamentals of ransomware are pretty simple, but the stress it causes when ransomware hits is anything but simple. Your best defense is to arm yourself with information, including how to prevent it and what to do if it infects your electronics.

What is ransomware?

Ransomware is a scam that targets your information. Rather than steal it, as with identity theft, the criminal holds it hostage by preventing you from accessing files on your computer or even shutting down entire systems. The crook sends you instructions on decrypting these files after he or she has been paid via cyber currency like Bitcoins.

How does it get into my computer?

Like many tech problems, the common culprits include visiting shady websites and/or engaging with phishing emails. The attempts to infect your computer—via an advertisement or seemingly-legitimate inquiries from friends and large companies—get more creative (and more believable) every day.

What do I do if ransomware strikes?

Becoming infected with ransomware is very scary. And the messages are designed to elicit as much fear as possible in targeted victims. Experts advise that you:

- **Don't pay the ransom.** But you want your information unlocked, right? Authorities at the federal level counsel victims that, just as the government doesn't negotiate with the bad guys in real life, you shouldn't do so with cyber criminals. That encourages thieves to re-target you (yep, it happens all the time) or someone else.
- **Hope there's a decryptor to help.** Companies have created programs that can decrypt some files hit by relatively unsophisticated ransomware. If the ransomware is cutting-edge, though, you're probably out of luck. And because there's risk in applying the wrong decryptor to your files, it's best to seek assistance from an IT expert.
- **Clean it up.** In the event that you don't get your files back (sigh…), you can still clean up the damage to avoid future threats from the same malware. Either you or a paid expert can download a program that essentially scrubs the ransomware from your computer.

How can I prevent it?

- **Bookmark your sites.** Some people land on websites that infect their computer by mistyping the web address of a legitimate site. To prevent that scenario, use the bookmark function to take you straight to trusted sites.
- **Verify emails.** Bad emails can lead to a host of problems, so learning to sift out the dangerous ones is crucial. To prevent ransomware attacks, always check the sender's address against a valid contact list before opening. And triple check before you click on or download anything contained in an email.
- **Security is supreme.** Ideally, you'll have layers of security that work together to catch malware at different points. At a minimum, make sure your security programs filter spam away from your "regular" email and are always up to date. Consider commercial-grade systems for even better protection.
- **Pay attention to your computer.** If you're diligent about monitoring your system, you may notice signs that it's been infected. The problem is that some of those signs—like a slowdown in operating speed—might not seem all that unusual. If you have a bad feeling, immediately shut down your computer and disconnect it from the internet. This "paralyzes" the ransomware, but you'll still need to install a security program to sweep it.

If your financial information has been compromised, F&M Bank may be able to help. We offer multiple resources to customers who've experienced cyber fraud.