Protecting You and Your Business

FCCB
FIRST CITIZENS COMMUNITY BANK

BUSINESS EMAIL IMPOSTERS

A scammer sets up an email address that looks like it's from your company. Then, the scammer sends out messages using that email address. This practice is called spoofing, and the scammer is what we call a business email imposter. Scammers do this to get passwords and bank account numbers or to get someone to send them money. When this happens, your company has a lot to lose. Customers and partners might lose trust and take their business elsewhere — and your business could then lose money.

How to protect your business:

1. Use email authentication. When you set up your business's email, make sure the email provider offers email authentication technology. That way, when you send an email from your company's server, the receiving servers can confirm that the email is really from you. If it's not, the receiving servers may block the email and foil a business email imposter.

2. Keep your security up to date. Always install the latest patches and updates. Set them to update automatically on your network. Look for additional means of protection, like intrusion prevention software, which checks your network for suspicious activity and sends you alerts if it finds any.

3. Train your staff. Teach them how to avoid phishing scams and show them some of the common ways attackers can infect computers and devices with malware. Include tips for spotting and protecting against cyber threats in your regular employee trainings and communications.

If someone spoofs your email:

1. Report it. Report the scam to local law enforcement, the FBI's Internet Crime Complaint Center at *IC3.gov*, and the FTC at *FTC.gov/ Complaint*.

2. Notify your customers. If you find out scammers are impersonating your business, tell your customers as soon as possible — by mail, email, or social media. If you email your customers, send an email without hyperlinks. You don't want your notification email to look like a phishing scam. Remind customers not to share any personal information through email or text. If your customers' data was stolen, direct them to *IdentityTheft.gov* to get a recovery plan.

3. Alert your staff. Use this experience to update your security practices and train your staff about cyber threats.