

OCTOBER 2022



ALBION  
FINANCIAL  
GROUP



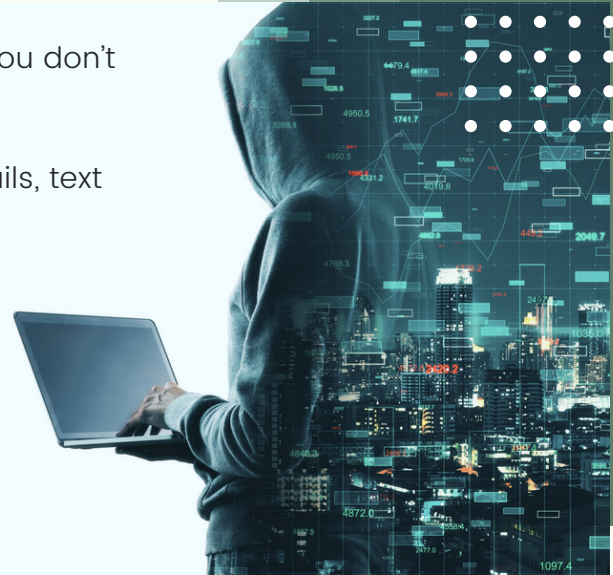
# INDIVIDUAL CYBERSECURITY

Fraud is on the rise. Scammers are getting smarter. We want to make it easy for you to learn more about cybersecurity and increase awareness about staying safe online.

# PHISHING

Cybercriminals like to go phishing, but you don't have to take the bait.

Phishing is when criminals use fake emails, text messages, social media posts or direct messages with the goal of luring you to click on a bad link or download a malicious attachment. If you click on a phishing link or file, you can hand over your personal information to the cybercriminals. A phishing scheme can also install malware onto your device.



No need to fear your inbox, though. Fortunately, it's easy to avoid a scam email, but only once you know what to look for. With some knowledge, you can outsmart the phishers every day.

## SEE IT SO YOU DON'T CLICK IT.

The signs can be subtle, but once you recognize a phishing attempt you can avoid falling for it. Here are some red flags to be on the lookout for:

- **Generic greetings** – Phishing emails sometimes include generic greetings, such as “Dear Sir or Madam” or “Dear Customer” rather than using the recipient’s name.
- **Personal information** – Bad actors leveraging phishing techniques may ask users for personal information. Most legitimate companies will never email customers and ask them to enter login credentials or other private information by clicking on a link to a website.
- **Urgent response** – Some phishing emails attempt to create a sense of urgency. For example, claiming that the recipient’s account is in jeopardy if they don’t act immediately.
- **Use fear** – Phishing emails will sometime claim there is a problem with one of your accounts – or that it is on hold – and then ask you to click on a link to make a payment or update some personal information to “correct the issue.”
- **Subtle misspellings** – The logo in the top corner appears to be legit, but the email account has a typo.

Now that you know how to spot a phishing email – how do you protect yourself?

- Slow down and review emails and texts carefully before clicking any links or downloading attachments.
- If the content of an email is concerning or seems suspicious, call the company in question using the phone number on the website (not the email) to find out if the email is legitimate.
- Be on the lookout for spoofed (fake or disguised) links. To check to see if a hyperlink in the message body leads to the page it claims, hover your cursor over the link to verify its authenticity before clicking.
- If the email sender is asking for sensitive information or requesting a financial transaction, verify the authenticity of the request via a known phone number or legitimate email address.
- Always be cautious about opening emails, clicking on links and downloading attachments from senders you do not recognize
- Don't click on a company's link in an email, type the site into your browser by hand.
- Be careful of what you post on social media. Bad actors will leverage information on social media to create targeted phishing attacks.

Ultimately, being overly cautious with emails can't hurt.

**When in doubt, throw it out:** Links in emails, text messages, social media posts and online advertising are often how cybercriminals try to steal your personal information. Even if you know the source, **if something looks suspicious, delete it.**

## CONTACT ALBION

If you receive a suspicious email, call or text claiming to be from Albion, let us know. We'll work with you to determine the legitimacy of any suspicious messages.

PHONE: (801) 487-3700

EMAIL: [CYBERSECURITY@ALBIONFINANCIAL.COM](mailto:CYBERSECURITY@ALBIONFINANCIAL.COM)

FOR MORE INFORMATION VISIT [ALBIONFINANCIAL.COM/LEARNING-CENTER/CYBERSECURITY/](https://ALBIONFINANCIAL.COM/LEARNING-CENTER/CYBERSECURITY/)

# MORE WAYS TO STAY SAFE

## Download a password manager

Duplicating passwords or using common passwords is a gift to hackers. If one account is compromised, a hacker will typically try the same username and password combination against other websites.

A secure password is your first line of defense in protecting your personal, private data as well as other sensitive company information. Complex passwords are much harder to guess, but they can also be a challenge to remember. The simplest, most secure way to manage unique passwords is through a password manager application. A password manager is software created to manage all your online credentials like usernames and passwords. Many are free. Often, browsers and device operating systems include password management programs. Password managers store your passwords in an encrypted database (think of it as your personal data vault). These programs also generate new passwords when you need them. Really, it has never been easier to safely generate, store and access your passwords.

## Use multi-factor authentication (MFA)

MFA will fortify your online accounts by enabling the strongest authentication tools available, such as biometrics or a unique one-time code sent to your phone or mobile device.

At least 15 billion passwords are for sale on the Dark Web. A second method of authentication provides extra protection even if a username and password is compromised. By adding one more simple step when logging into an account, multi-factor authentication greatly increases the security of your account.



# THANK YOU

WE DO NOT TAKE  
LIGHTLY THE TRUST  
YOU HAVE PLACED  
IN US.

Albion Financial Group is committed to maintaining the confidentiality, integrity and security of the personal information that is entrusted to us. Protecting our clients' identity is of the utmost importance. We will never send you an email asking for your account information.

We do not provide your personal information to mailing list vendors or solicitors and we regularly review the importance and methods of maintaining client confidentiality with our entire staff.

