

Information Security Best Practices



DISCLAIMER

The purpose of this session is to provide helpful information on the subject matter covered. It is offered with the understanding that Pinnacle Bank (“Pinnacle”) is not rendering any type of professional advice and is simply providing resources of what to consider. You should additionally seek the services of a competent professional regarding your personal situation.

The information provided is intended to offer general tips on security issues and social engineering scenarios. Pinnacle does not guarantee the effectiveness of these tips in preventing security threats. Clients are encouraged to stay vigilant and regularly update and assess its security measures. Clients are encouraged to independently verify the best security practices for its individual companies and businesses and implement best practices for security its environment and networks and training from a professional in the security and vulnerability management profession.

Use of the information provided is educational and informational. Pinnacle shall not be held liable or responsible for any losses due to client’s failure to adhere to any type of security practices.





- 43% of cyber attacks target small businesses.
- 41% of small businesses fell victim to a cyber attack in 2023.
- Average cost of a data breach in 2023 \$9.48M.
- 83% are not financially prepared to recover from an attack.
- Only 50% recovered their data.
- 27% of the time, hackers made additional demands for money.
- 1 in 323 emails sent to small businesses are malicious.
- 54% of small businesses don't have a response plan.
- 50% of small and mid-sized businesses reported suffering at least one cyber attack in the last year.
- ***60% of businesses close within 6 months of an attack.***

Business Email Compromise Example



Hi Ken,

See the attached wiring instructions to receive all closing funds. Your cash-to-close final amount is **\$350,566.27**.

NOTE : For any excess funds, we would give you a check back for any overages at closing.

Please advise when the transfer is complete so I can watch for it and finalize your closing documents.

Let me know if you need anything else.

Teresa Parsons
Hollers and Atkinson, P. C.
110 N. Main Street
Troy, NC 27371
(385) 226-5117

HOLLERS & ATKINSON, P.C.

110 NORTH MAIN STREET
TROY, NORTH CAROLINA 27371

RUSSELL J. HOLLERS (retired)

CARL W. ATKINSON, JR. (retired)

RUSSELL J. HOLLERS, III

(864) 573-7566 fax

Instructions for wiring funds to Hollers & Atkinson, P.C.

Receiving Bank: Huntington Bank 420 Davis Ave, Elkins, WV 26241
ABA Routing #: 044000024

Credit

Hollers and Atkinson, P. C. (Trust Account)
110 N. Main Street Troy, NC 27371
Account Number: 01640125137

*****PLEASE PUT OUR CLIENT'S NAME ON THE WIRE*****

--NOTICE--

**NO CHECKS WILL BE ACCEPTED
FOR LOAN PROCEEDS**

--LENDERS MUST WIRE ALL LOAN PROCEEDS--

Business Email Compromise Example



#7: Opportunist siphons \$793,000 in new construction funds for N.C. church

What happened: Elkin Valley Baptist Church in North Carolina spent a decade collecting \$1.5 million to build a new worship center. In late 2022, when they were ready to break ground on the project, bad actors swooped in to launch a BEC campaign that led to the [theft of more than half of the construction fund](#).

BEC strategy: On a Friday night, two emails arrived in the church's financial secretary's inbox. One was sent by the builder with a request for the first half of the payment and transfer instructions. The other email with different transfer details was fraudulent—but almost identical to first. It even included the previous email thread in the body of the message. Unfortunately, a church representative believed it was legit and sent the payment to the fraudsters on Monday.

Progressive Legal Group

PROGRESSIVE LEGAL GROUP
OFFICIAL BUSINESS
2304 W. HEFNER RD # 21480
OKLAHOMA CITY, OK 73120

CIVIL LAWSUIT NOTIFICATION

Creditor: EZMONEY
Type: INSTALLMENT LOAN
Additional Activity: NSF FRAUD
SSN: [REDACTED]
Defendant: MELISSA [REDACTED]
File No.: 8233495356
Amount Due: \$1,567.53
Due Date: January 23, 2024

RESPONDENT

MELISSA [REDACTED]
[REDACTED]
[REDACTED]

Please note that this debt was incurred several years ago

For questions, please call:
1-800-391-7635

Visit us online: www.ProgressiveLG.com

NOTIFICATION OF LAWSUIT & CIVIL COMPLAINT

Dear MELISSA [REDACTED] 12nd notice

This letter is to inform you that due to the severe delinquency of your previous installment loan originating with EZMONEY (a subsidiary of EZCORP) while working at or for WACHOVIA BANK, NA, we are now reviewing your account for immediate legal action (filing a lawsuit) against you, of which would result in a civil court judgment. A civil judgment will immediately be reported to the credit bureaus and will be aggressively enforced. In addition to the current balance owing on your account, any back interest, court costs and attorney fees will be added to this debt and the total amount sought in a lawsuit.

Civil judgments generally result in a wage garnishment and/or lien against personal property or bank account, depending on the applicable form of enforcement allowed by state law. Criminal charges are not usually pursued in civil court.

CAUSE OF ACTION TWO (2): Because you obtained this loan and immediately closed or changed your bank account, and because your check (ACH payment) was returned unpaid by your bank due to non-sufficient funds (NSF) for an amount greater than \$100.00, we have noted your case with fraudulent activity and with a malicious intent to commit wire fraud.

We further reserve the right to subpoena the following reference(s) listed on the original application as witnesses to testify against you should this matter go to trial:
KENNETH [REDACTED] KATHRYN [REDACTED]

It is very important that you pay the outstanding balance owing on your account no later than the due date referenced above. If you mail your payment, please be sure to allow enough mailing time to ensure that your payment is received by our office prior to your due date. If your payment is not received by our office by the due date, or if we do not hear from you, our intent is to immediately have you served a court summons by the Guilford County Sheriff's Office to appear in civil court for further action.

To pay online now, or to check the status of your case, please visit us at www.ProgressiveLG.com, or call us at 1-800-391-7635.

Cc: U.S. District Court, Guilford
Transunion credit bureau

Your Credit Score: [REDACTED]



During this process, our intent is to run your credit report which will result in a hard inquiry being reported to the credit bureaus. A hard inquiry will significantly impact your credit score.

RE: EZMONEY
File #: 8233495356
Amount Due: \$1,567.53

Detach and Return With Your Payment



Make payable to:

MELISSA [REDACTED]
[REDACTED]

PROGRESSIVE LEGAL GROUP
2304 W. HEFNER RD # 21480
OKLAHOMA CITY, OK 73120

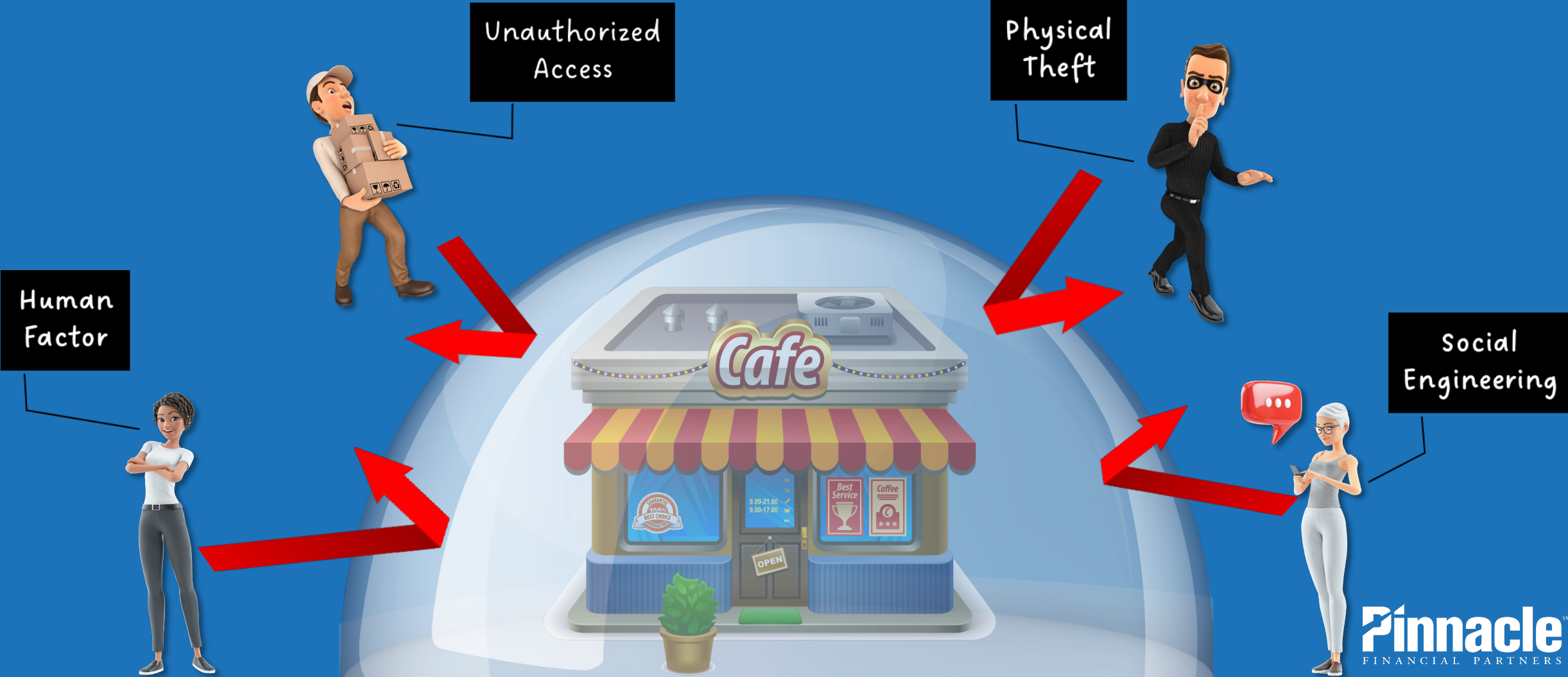
This is an attempt to collect a debt, and any information obtained will be used for that purpose. A final determination to take legal action will be made on your due date should your payment not be received by our office, and after which time we have thoroughly reviewed your file to ensure any legal proceedings are in accordance with state law.





Meet Hushpuppi

What are you protecting from?





Human Factor

- 95% of cybersecurity breaches are caused by human error.
 - Weak passwords or poor password hygiene.
 - Falling victim social engineering schemes.
 - Rushing, making mistakes, taking shortcuts.
- Pain-In-The-Butt test. If it's a pain, it's probably worth doing.
- Avg. person has 240 online accts & reuses passwords 14 times.
- The bigger the company, the higher the risk.
- Require secure passwords and multi-factor authentication.



Unauthorized Access

- Limit employee access to relevant files and areas (military).
- Restrict sensitive information to trusted, top-level employees, this includes online banking, wire transfers, credit cards, etc.
- Be on alert for unauthorized/unknown visitors.
- If possible, lock down USB ports.
- Limit contractor access, (Target \$202MM).



Physical Theft

- Check Washing
- Documents left on desk, copier/printer or in recycle bucket.
 - Client information
 - Credit Card Statements
- Lock computer when walking away.
- Lost/stolen company laptops/phones (Use VDI).
- USB drives and file sharing sites.
- Disgruntled employees



Social Engineering

- Manipulation to divulge sensitive information or perform a task.
- Phishing- email attack vector for cyber criminals.
 - “We changed banks. Please update our account info”.
- Smishing- text message attack vector for cyber criminals.
 - CEO Fraud
- Vishing- voice attack vector for cyber criminals.
 - Never rely on Caller-ID as proof of identity.
- Quishing- QR code attack redirecting victims to malicious websites or prompting them to download harmful content.
- Free Wi-Fi (Use VPN)

Text Scam Examples

MSG from USPS

We are holding a package that needs to be delivered, due to an incorrect delivery address.

<https://uspostalinfo.com/update>

MSG from USPS

We are holding a package that needs to be delivered, due to insufficient postage.

<https://uspostalinfo.com/update>

Thank you for your recent visit to CVS. Please tell us how we did. Complete the survey for a \$50 gift card.

<https://cvssurvey.com/giftcard>

Steps to Mitigate Risk

1

Start a Campaign

Teams must be formally trained and routinely reminded of:

- the significance of the threat
- your level of commitment
- the tasks they need to perform (turn on MFA, update their software) and avoiding phishing)
- recognizing social engineering schemes
- how to escalate suspicious activity
- new trends(USB charging)

2

Develop a Plan

What happens at the first sign of a cyber incident? Does everyone know what to do? Will they react without direction? Consider:

- Select an external partner
- Create policies and proc. for access controls, acceptable use, etc.
- Roles for your team, incl. an incident manager
- Communication plan
- Document postmortem process (blameless)
- Routinely review the plan

3

Test your Team

Don't wait until an event. Everyone needs to understand:

- Phishing Tests
 - Stranger Danger
 - Pop in to empty offices
 - Locked PCs
 - Documents
 - Tailgating
 - Tabletop Exercises
- Building strong habits takes time. Practice *blameless accountability*. Correct bad behaviors, reward good behaviors and set goals.

4

Protect your Business

- Positive Pay with Payee Match.
- ACH Block and ACH Filter.
- Cyber insurance provides coverage that protects your business and you personally against damages in the event of a cyberattack. It can also provide coverage that protects your business against damages incurred by clients, vendors and others.



ShieldsUp

Prepare for, respond to, and mitigate the impact of cyberattacks.

[LEARN MORE](#) →



SECURE BY DESIGN

Shifting the Balance of Cybersecurity Risk: Principles and Approaches for Secure by Design Software. Read the updated guidance NOW!

[LEARN MORE](#) →

Use Independent Resources



Steps to Mitigate Risk

1

Start a Campaign

Teams must be formally trained and routinely reminded of:

- the significance of the threat
- your level of commitment
- the tasks they need to perform (turn on MFA, update their software) and avoiding phishing)
- recognizing social engineering schemes
- how to escalate suspicious activity
- new trends(USB charging)

2

Develop a Plan

What happens at the first sign of a cyber incident? Does everyone know what to do? Will they react without direction? Consider:

- Select an external partner
- Create policies and proc. for access controls, acceptable use, etc.
- Roles for your team, incl. an incident manager
- Communication plan
- Document postmortem process (blameless)
- Routinely review the plan

3

Test your Team

Don't wait until an event. Everyone needs to understand:

- Phishing Tests
 - Stranger Danger
 - Pop in to empty offices
 - Locked PCs
 - Documents
 - Tailgating
 - Tabletop Exercises
- Building strong habits takes time. Practice *blameless accountability*. Correct bad behaviors, reward good behaviors and set goals.

4

Protect your Business

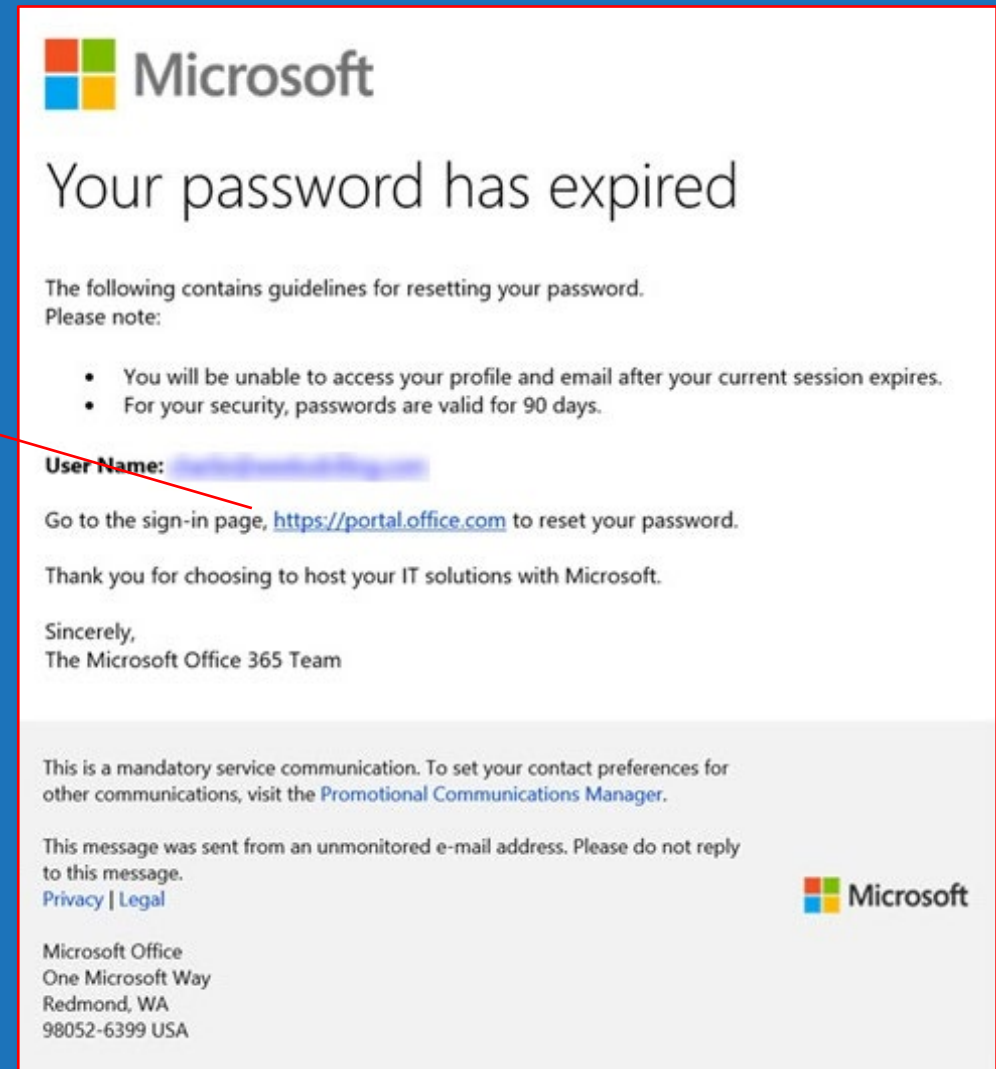
- Positive Pay with Payee Match.
- ACH Block and ACH Filter.
- Cyber insurance provides coverage that protects your business and you personally against damages in the event of a cyberattack. It can also provide coverage that protects your business against damages incurred by clients, vendors and others.

Most Abused Brands?

```
http://portal.microsfonline.com/?  
wa=wsignin1.  
0&rpsnv=4&ct=1453814382&rver=6.6.  
6556.  
0&wp=mbi_ssl&wreply=&cbcxt=out&id=y  
2hhcmxpzub3zwwrc2ryawxsaw5nlmnbq=
```

- Microsoft (30M)
- Amazon (6.5M)
- DocuSign (3.6M)
- Google (2.6M)
- DHL (2M)
- Adobe (1.5M)

Don't assume it is
from them, even if it
has their logo
(including Pinnacle)!



The screenshot shows an email from Microsoft with the subject "Your password has expired". The email body contains the Microsoft logo, the subject line, a warning that the user will be unable to access their profile and email after the current session expires, and a note that passwords are valid for 90 days. It includes a "User Name:" field with a redacted name, a link to the sign-in page (<https://portal.office.com>), and a thank you message from the Microsoft Office 365 Team. At the bottom, there is a footer with the Microsoft logo, a disclaimer that the message is a mandatory service communication, and contact information for Microsoft Office in Redmond, WA.

www.pinnacle.com
www.pinnacle.com

What to look for?

Focus on the emails with links and attachments.

- Does the email create a sense of urgency?
- Should this have gone to my personal email?
- Spelling/grammar errors; CAPS, !!; formatting inconsistencies?
- Examine the link by hovering. Seem sketchy? This is a safe link.
- Trust your gut!

