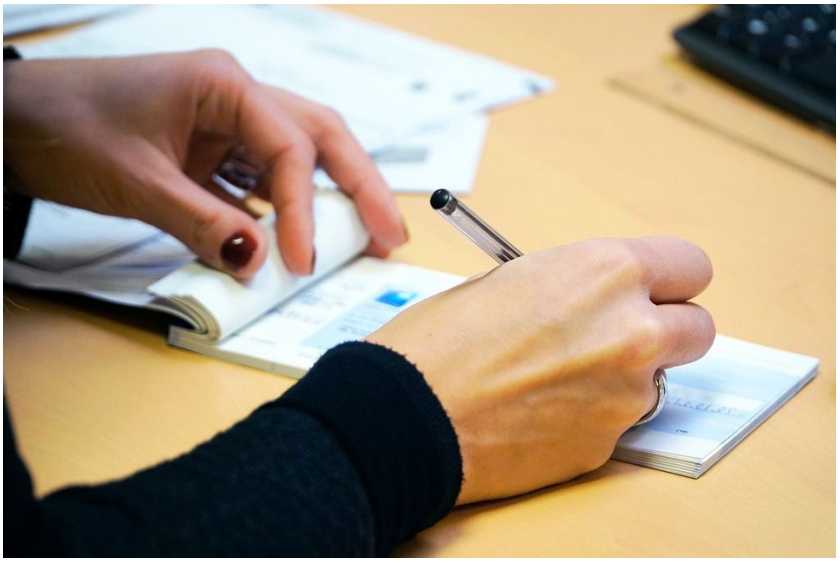
Fortified Data Security Services.
All layers. All levels.

Business is Hard Enough w/o Sending a Hacker $40k+



There's nothing worse than getting a call from a vendor wondering why you haven't sent a check for their last statement.

You say: "But you emailed back to do an ACH transfer because we're having check processing issues."
They say: "No I did not. We take checks as always."
You say: "But you sent us the ACH bank information from your account to make a payment."
They say: "No, I did not."

This is when the uncertainty and panic starts to set in. You're not understanding what just happened. They didn't get the money and you no longer have it. You call the sheriff and they give you a report. They laugh when you ask what they're going to do about it. You inquire, "What about the FBI?" But the laughter continues.

You start to investigate. While looking at emails, you discover that once the statement was sent by the true vendor's email account, the next one stating having "check cashing issues" was from a similar but different domain. The vendor's domain is alwayscheck.com but the spoofing domain was allwayscheck.com, and you didn't notice. Law enforcement will not help. Insurance will not help even with cyber security insurance, unless you have a specific rider for this situation. IT can help determine what, where and how it happens. At this point it is a forgone conclusion. The money is lost.

So what likely happened? The concept for this is that one's email gets compromised at either (or both) ends of a conversation. Access for forwarding of these emails can be via a compromised mail server, local PCs, and hosted email services. The hacker monitors these vulnerabilities, looking for key words or situations to take advantage of. They may have been watching for months before something worthwhile comes along.

Well, in this instance, we only had access to one side of the equation. But SkyPort has steps to follow in order to begin the remediation process.

The goal of these first steps is to minimize the risk of further fraud.

- In this case, the client is using Office 365.
    - Change all account Domain/Email/Hosted Services passwords including the admin's
    - Review email server or hosted services and check
        - Mail flow rules
        - Mailbox delegations
        - Rouge accounts
        - Forwards
        - Aliases
        - Audit Logs
        - Keyloggers
        - Remote access
        - Virus/Malware

    - Review Workstations
        - Forwarding Rules in Client
        - Keyloggers
        - Remote access
        - Virus/Malware

You now need multiple layers of protection to be safe. One of the most important and most ignored layers is user training. Training goes over what to look for in cyber, physical and hybrid social engineering attacks.

We have provided organizations with on-site physical social engineering testing. We test their current training and then present the results to improve the areas of concern. In our test we have gotten full access to systems, including the administrative password for an entire IT infrastructure. At one location, it was easy to find sticky notes everywhere containing sensitive login information.

It's not the fault of the end-users who have not been properly trained. It is in people's nature to help others, assume good intent and avoid conflict. It's perfectly okay to trust, but it is extremely important to verify, verify and verify again. Be the detective, ask questions, ask for proof, check with others, call known numbers to verify access or any request. Stop, think and be safe.