新世界时报
www.newworldtimes.us
二零二四年五月三日 星期五 Friday, May 3, 2024

全美小企业周:国税局提醒小企业主小心数据安全,保护他们的企业、员工和客户

华府 — 在全美小企业周继续开展之际,美国国税局敦促小企业主落实数据安全保障措施,保护他们的财务、个人和员工信息免受诈骗和网络犯罪分子的追捕。

国税局不断发现小企业和其他人面临各种与金融和身份盗窃相关的骗局,这些骗局试图获取可用于提交虚假小企业税表、打劫商业银行账户和创建被盗身份的信息。

例如,"网络钓鱼"和"鱼叉式网络钓鱼"诈骗继续针对小企业以及税务专业人士和个人纳税人。小型企业仍然是 W-2 表格诈骗的目标,身份窃贼试图诱骗公司领导者分享敏感数据。

"每年,美国国税局发现有数千起试图攻击小企业主和其他纳税人的尝试。这些骗局的受害者可能会面临严重的财务后果。"国税局局长 Danny Werfel 表示,"网络犯罪分子是无情的,任何人都可能成为目标。企业主和个人保护自己的最佳方法是充分了解最新的骗局,持续保护他们的计算机和智能手机,并在家里和公司安装数据安全装置以保护敏感信息。"

网络犯罪分子全年无休

数据盗窃和网络攻击是全球性威胁,它们可以在白天或晚上的任何时间利用诈骗和欺诈计划来伤害个人和小型企业。网络犯罪分子非常擅长掩盖自己的踪迹,并且可以隐藏在世界任何地方。

他们利用人类行为模式和计算机系统窃取财务和个人信息并诱骗受害者。如果小型企业不能正确保护其计算机系统并对其员工进行智能数据保护实践培训,则所有者很容易成为想要闯入银行账户和窃取身份的不良行为者的目标。

国税局敦促小型企业界认真对待网络犯罪的威胁,并了解保护其业务数据免遭身份盗窃的重要性。他们应该采用强大的技术工具和服务来严格保护金融和贸易信息,并保护与客户、员工和业务合作伙伴直接相关的数据。

网络犯罪分子不断寻找可利用的弱点。小企业主通过实施基本的网络安全措施和培训员工,可以显著降低遭受代价高昂的攻击的风险。这些攻击可以针对企业最有价值的数据,包括:

- 信用卡和付款信息。数据泄露可能会损害企业的声誉,并使所有者承担欺诈费用。
- 企业和员工身份。被盗信息可用于多种犯罪,包括身份盗窃和欺诈。
- 税务和财务信息。黑客可以利用这些信息提交欺诈性税表,从而花费企业主的时间和金钱来解决问题。

为了保护商业投资、客户和员工,小企业主尽早采取基本的网络安全措施并保持警惕,掌握有关最新诈骗的信息。

诈骗者如何瞄准受害者:骗局、骗局和更多骗局

欺诈者和网络犯罪分子是操纵人类行为的投机分子。他们利用潜在受害者与他人进行社交互动和交流的自然愿望,窃取数据和身份。欺诈者使用电子邮件、短信和社交媒体等常见技术,通过一次性向数千个目标发送消息来直接窃取个人信息,或者让受害者点击嵌入的链接或附件,从而进行"网络钓鱼"。

使用电子邮件作为通过"网络钓鱼"操纵行为的方法仍然是盗贼寻找潜在受害者的常用策略。小型企业应对与税务相关的"网络钓鱼"电子邮件诈骗保持警惕,这些诈骗通常可以巧妙地编写来欺骗员工打开有害的嵌入式链接或附件。我们鼓励小型企业和消费者将与国税局相关的诈骗邮件发送至 phishing@irs.gov。

W-2 表格盗窃骗局就是这样的一个例子。虽然这些骗局的操作随着时间的推移而演变和变化,但在最常见的操作中,窃贼冒充公司高级管理人员,向薪资员工发送电子邮件,要求提供员工名单及其 W-2,其中包含敏感的税务和财务信息数据。随着这些骗局变得越来越复杂,小企业可能不会意识到自己已经成为税务骗局的受害者,直到开始出现带有员工姓名的欺诈性税表。

对于遇到 W-2 骗局的雇主,有特殊的报告程序。请访问身份盗窃中心的商业部分(英文)以获取更多信息。

肮脏十二条骗术

国税局每年都会发布"肮脏十二条骗术",列出了威胁小企业和其他纳税人的普遍存在的诈骗和欺诈计划。这些威胁包括员工留任税收抵免(ERC)可疑申请的不择手段和激进推广人。

这些可疑的员工留任税收抵免申请常常使毫无戒心的企业和其它实体面临处罚、利息,甚至可能因在不符合资格且无权获得员工留任税收抵免的情况下申请而面临刑事起诉。

如果个人或小企业主怀疑自己可能成为受害者,可以参考"肮脏十二条骗术"中提供的信息。例如,企业仍然可以选择撤回任何未处理的可疑员工留任税收抵免申请,并应针对尚未支付的任何纳税期迅速进行申请撤回程序(英文)。

企业主可以将"肮脏十二条骗术"作为其自行研究的起点,进而从其它可信来源了解各种流行骗局。

目前,"肮脏十二条骗术"报告的影响小型企业的最严重诈骗之一是"新客户""鱼叉式网络钓鱼"骗局。鱼叉式网络钓鱼通过恶意电子邮件或短信针对特定个人、组织或企业。

在"新客户"骗局中,网络犯罪分子向已知税务专业人士或企业主展示自己是新的潜在客户,要求他们回复电子邮件。如果不知情的代报税人或企业主做出回复,犯罪分子就会发送恶意附件或网站地址,这些附件或网站地址可能会危害受害者的计算机系统,并允许攻击者访问敏感的客户和财务信息。以下是一些需要注意的危险信号:

- 语法上的奇怪之处。写得不好、用词不寻常的电子邮件是一个严重的危险信号。
- 可疑的请求。在验证发件人的合法性之前,企业主应始终警惕任何异常请求或共享信息。
- 欺骗性电子邮件。诈骗者可以模仿以前的客户电子邮件,使它们看起来很真实。不要被愚弄,请另外独立验证发件人的地址。

通过保持警惕并了解这些骗术,小企业主可以保护自己及其客户免受"新客户"骗局的伤害。谨慎总是比妥协好。

不要成为容易的目标,学习网络安全基础知识

强烈鼓励小企业主尽可能多地了解网络安全最佳实践,即使日常信息技术保护是外包的。美国国税局建议企业主实施美国联邦贸易委员会发布的最佳实践(英文)。许多人都熟悉常识性的习惯和技巧,但不要认为它们是理所当然的。适用于家庭的方法也适用于企业。

保护企业文件和设备:

- 更新软件。这包括应用程序、网络浏览器和计算机操作系统。设置为自动更新。
- 保护业务文件。离线、外部硬盘或云中备份重要文件。还要确保安全地存储纸质文件。
- 设置密码。对所有笔记本电脑、平板电脑和智能手机使用密码。不要将这些设备留在公共场所无人看管。
- 加密设备。加密包含敏感个人信息的设备和其他媒体。这包括笔记本电脑、平板电脑、智能手机、可移动驱动器、备份磁带和云存储解决方案。
- 使用多重身份验证。需要多重身份验证才能访问包含敏感信息的网络区域。除了使用密码登录之外,这还需要其他步骤,例如智能手机上的临时代码或插入计算机的密钥。

保护企业无线网络:

- 保护企业路由器的安全。设置路由器后,更改默认名称和密码、关闭远程管理并注销管理员身份。
- 至少使用 WPA2 加密。确保路由器提供 WPA2 或 WPA3 加密并且加密设置已打开。加密可保护通过网络发送的信息,使其无法被外部人员读取。

让智能安全成为常规措施:

- 需要强密码。强密码至少由 12 个字符组成,由数字、符号、大小写字母组成。切勿重复使用密码,也不要通过电话、短信或电子邮件分享密码。限制登录尝试失败的次数,以限制密码猜测攻击。
- 培训员工。通过实施定期的员工培训计划来创建安全文化。随时了解最新的数据安全风险和漏洞,并让员工随时了解情况。考虑阻止无视数据安全措施和培训的员工访问网络。
- 设置一个计划。制定保存数据、运营业务并在发生数据泄露时通知客户的计划。美国联邦贸易委员会的数据泄露响应:企业指南(英文)提供了企业主在发生网络泄露时可以采取的步骤。

有关企业主如何保护其投资、客户和员工免受网络犯罪分子侵害的更多信息,请访问 FTC 的小型企业网络安全(英文)。

如果小型企业成为身份盗窃的受害者,下一步该怎么办

国税局还发布了《表格 14039-B,企业身份盗窃宣誓书》(英文),使小型企业可以在电子提交的税表被拒绝等情况下主动向国税局报告可能的身份盗窃行为。如果小型企业收到以下信息,则应提交表格 14039-B:

- 收到通知说以电子方式提交的税表被拒绝,因为同一时期的税表已申报。
- 收到通知涉及已提交的税表,但实体未提交该税表。
- 收到通知涉及向社会安全局提交的 W-2 表格,但该实体未提交该表格。
- 收到欠余额通知,而该实体并未欠余额。

如果小企业主成为税务欺诈的目标,国税局会提供 14039-B 表格来帮助快速解决问题。该表格使国税局能够简化沟通并更快地解决问题。但是,如果小型企业是数据泄露的受害者且没有税务相关影响,则不应使用 14039-B 表格。有关更多详细信息,请参阅身份盗窃中心的企业部分。

国税局还敦促小企业主及时更新其雇主身份识别号码 (EIN) 申请信息。地址或责任方的变更可以使用《表格 8822-B, 地址或责任方变更 - 企业》(英文)来报告。责任方的变更必须在 60 天内向国税局报告。当前信息可以帮助美国国税局找到解决身份盗窃和其他问题的联系人。

报告鱼叉式网络钓鱼和其它诈骗

企业主应立即报告诈骗,将可疑电子邮件或短信副本作为附件发送至 phishing@irs.gov。该报告应包括发件人的电子邮件地址、呼叫者的电话号码、日期、时间以及收到消息的电话号码或电子邮件地址。

IRS.gov 的报告网络钓鱼和在线诈骗页面提供了有关注意事项以及如何报告网络钓鱼和诈骗的更多信息。

纳税人还可以向财政部税务行政监察长(英文)或互联网犯罪投诉中心(英文)举报诈骗行为。另一个有用的工具是联邦通信委员会的智能手机安全检查器(英文)。

企业主和个人根据所涉及的骗局,也可以将信息发送给国税局检举人办公室(英文),以获得可能的金钱奖励。

报告诈骗有助于识别新出现的威胁。欺诈执法办公室(英文)的新兴威胁缓解团队与内部和外部利益相关者合作,识别和缓解对税务管理的威胁。

要报告滥用型推广人和代报税人,请填写在线《表格 14242 - 报告涉嫌滥用型税务推广或代报税人》(英文),或将填妥的表格 14242(英文)和任何支持材料邮寄或传真至推广人调查办公室的国税局领导发展中心。

邮件:

Internal Revenue Service Lead Development Center

Stop MS5040

24000 Avila Road

Laguna Niguel, California 92677 3405

传真: 877-477-9135

纳税人和税务专业人士也可以将此信息提交给国税局检举人办公室(英文),在那里他们可能有资格获得奖励。有关详细信息,请参阅滥用型税收骗局滥用型代报税人(英文)的部分。

有关更广泛主题的更多信息以及小型企业税务问题的答案,请访问 IRS.gov。