# from AARP

If you haven't already received your new EMV "smart chip" **credit card(s)**, you soon will. What else can you expect, even if you were previously sent the new plastic? Expect bogus emails allegedly sent by card issuers, PayPal or other businesses that supposedly provide details about your account with more secure, chip-imbedded cards.

It's a new incentive for old tricks to install **computer malware** and/or **phish** for account information and log-in credentials.

Why now? Oct. 1 is the deadline set by Visa, MasterCard, American Express and Discover for the so-called "liability shift." That's when fraudulent charges currently eaten by **credit card** companies move to either the banks and credit unions issuing credit cards or the merchants accepting them — whichever party is deemed "least EMV-compliant." For instance, if a retailer has updated its point-of-sale terminals to accept chip-embedded cards but the card-issuing bank lags in implementing transaction-supporting technology, the bank is held liable for the fraud.

Although millions of EMV cards (short for Europay, MasterCard and Visa) have already been issued, there's now a big push to quickly deliver the remaining plastic imbedded with a small computer chip; it's that small, metallic square on the front of EMV cards that creates a unique transaction code that cannot be used again, unlike magnetic-stripe cards that store unchanging account details that aid fraudsters.

And that push — now through year's end, when most, if not all, EMV plastic reaches cardholders — means opportunity for scam emails. Some are already circulating, so **here's what you should know:**

**1.** Legitimate emails from card issuers should be short, to-the-point notifications that your new EMV card is being mailed, perhaps with an "expect within 10 days" time frame. They should not include links or attachments promising details or urging action to "update your account" or the like; that's the calling card of scammers.

As a general rule, don't trust links in emails — and before clicking, always hover your computer mouse over the link; if it doesn't display the sender's company name, assume the worst. It's also safer to access any business website by typing its URL yourself, not via provided links. Or call the phone number listed on your card, not provided in emails.

**2.** Bogus PayPal emails are making the rounds, with malware-laden "Update Your Account" attachments. **Legit PayPal emails never include attachments**.

**3.** Authentic emails from card issuers will address you by name and include some specific reference to your credit card, such as the last four digits of your account number. Those from PayPal, eBay or other businesses will also include your name. Emails vaguely addressed to Dear “Cardholder,” “Customer” or “Account Holder” are scams.

**4.** Even if the email includes your name, don’t trust it unless you previously provided your email address to that business (for instance, when you enrolled in online banking). Email mailing lists — with account holder names — can be purchased by scammers.

**5.** Be suspicious of phone calls or text messages supposedly from card issuers about EMV cards. These could be “**vishing**” (for voice phishing) or “**smishing**” (named after SMS technology that sends text messages) attempts aiming to glean account and personal information.

**********